Learning Linux binary analysis

Type de contenu : Texte

Titre(s) : Learning Linux binary analysis [texte imprimé] : uncover the secrets of Linux binary analysis with this handy guide / Ryan elfmaster O'Neill

Auteur(s) : O'Neill, Ryan

Editeur, producteur : Birmingham, UK : Packt publishing, 2016

Description matérielle : 1 vol. (XIII-253 p.) ; 24 cm

ISBN : 978-1-78216-710-5

Résumé ou extrait : [This book] will start by taking you through UNIX/Linux objects utilities, and will move on to teaching you about the ELF binary format. 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 use 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 analyzing static code. Finally, you will be walked through complex userspace memory infection analysis. (source : 4ème de couverture)

Sujet(s) : Linux
Linux (système d'exploitation des ordinateurs)
Systèmes d'exploitation (ordinateurs)