



Defect

→
Detect

Linux

Core Dump Analysis

Accelerated

Second Edition
Revised and Extended

Dmitry Vostokov
Software Diagnostics Services

Accelerated Linux Core Dump Analysis: Training Course Transcript with GDB and WinDbg Practice Exercises, Second Edition, Revised and Extended

Published by OpenTask, Republic of Ireland

Copyright © 2022 by OpenTask

Copyright © 2022 by Software Diagnostics Services

Copyright © 2022 by Dmitry Vostokov

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of the publisher.

Product and company names mentioned in this book may be trademarks of their owners.

OpenTask books and magazines are available through booksellers and distributors worldwide. For further information or comments send requests to press@opentask.com.

A CIP catalog record for this book is available from the British Library.

ISBN-13: 978-1-912636-79-2 (Paperback)

Revision 2.5 (July 2022)

Contents

About the Author.....	7
Presentation Slides and Transcript.....	9
Core Dump Collection.....	31
Practice Exercises	41
Exercise 0 (x64, GDB).....	46
Exercise 0 (A64, WinDbg Preview, WinDbg, Docker)	48
Exercise A1 (x64, GDB)	64
Exercise A1 (A64, WinDbg Preview)	76
Exercise A2D (x64, GDB)	93
Exercise A2D (A64, WinDbg Preview).....	97
Exercise A2C (x64, GDB)	101
Exercise A2C (A64, WinDbg Preview)	104
Exercise A2S (x64, GDB).....	109
Exercise A3 (x64, GDB)	113
Exercise A3 (A64, WinDbg Preview)	116
Exercise A4 (x64, GDB)	121
Exercise A4 (A64, WinDbg Preview)	127
Exercise A5 (x64, GDB)	134
Exercise A5 (A64, WinDbg Preview)	137
Exercise A6 (x64, GDB)	142
Exercise A6 (A64, WinDbg Preview)	157
Exercise A7 (x64, GDB)	184
Exercise A8 (x64, GDB)	190
Exercise A8 (A64, WinDbg Preview)	205
Exercise A9 (x64, GDB)	229
Exercise A9 (A64, WinDbg Preview)	244
Exercise A10 (x64, GDB)	258
Exercise A10 (A64, WinDbg Preview)	271
Exercise A11 (x64, GDB)	280
Exercise A11 (A64, WinDbg Preview)	289
Exercise A12 (x64, GDB)	297
Exercise A12 (A64, WinDbg Preview)	307
Exercise K1 (x64, GDB).....	317

Exercise K2 (x64, GDB).....	367
Exercise K3 (x64, GDB).....	382
Exercise K4 (x64, GDB).....	395
Exercise K5 (x64, GDB).....	420
Selected Q&A.....	429
App Source Code	435
App0	437
App1	438
App2D.....	439
App2C	441
App2S.....	443
App3	445
App4	447
App5	449
App6	451
App7	453
App8	455
App9	458
App10	460
App11 / App12.....	462
K2.....	464
K3.....	465
K4.....	467
K5.....	469
Selected Analysis Patterns.....	471
NULL Pointer (Data).....	473
Incomplete Stack Trace	474
Stack Trace.....	475
NULL Pointer (Code).....	476
Spiking Thread	477
Dynamic Memory Corruption (Process Heap).....	478
Execution Residue (User Space)	479
Coincidental Symbolic Information	481
Stack Overflow (User Mode)	482
Divide by Zero (User Mode).....	483

Local Buffer Overflow (User Space).....	484
C++ Exception	485
Paratext	486
Active Thread.....	488
Lateral Damage.....	489
Critical Region.....	490