

Gerard Johansen

Digital Forensics and Incident Response

An intelligent way to respond to attacks



FOR SALE IN INDIA ONLY

Packt>

Digital Forensics and Incident Response

An intelligent way to respond to attacks

Gerard Johansen



Packt

BIRMINGHAM - MUMBAI

Digital Forensics and Incident Response

Copyright © 2017 Packt Publishing

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, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: July 2017

Production reference: 1210717

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-78728-868-3

www.packtpub.com

Credits

Author

Gerard Johansen

Copy Editor

Safis Editing

Reviewer

Nicole L. Stoneman

Project Coordinator

Judie Jose

Acquisition Editor

Rahul Nair

Proofreader

Safis Editing

Content Development Editor

Abhishek Jadhav

Indexer

Aishwarya Gangawane

Technical Editor

Manish D Shanbhag

Graphics

Kirk D'Penha

Production Coordinator

Aparna Bhagat

About the Author

Gerard Johansen is an information security professional with over a decade of experience in such areas as penetration testing, vulnerability management, threat assessment modeling, and incident response. Beginning his information security career while a cybercrime investigator, Gerard has built on that experience while working as a consultant and security analyst for clients and organizations ranging from healthcare to finance. Gerard is a graduate of Norwich University's Masters of Science in Information Assurance and a Certified Information Systems Security Professional.

Gerard is currently employed as an Enterprise Security Manager with a large retailer with a focus on incident detection, response and threat intelligence integration. He has also contributed to several online publications focused on various aspects of penetration testing.

About the Reviewer

Nicole L. Stoneman is the Director of Digital of Forensics at Vestigant. Ms. Stoneman has been conducting computer forensic exams since 2005 and has been involved in thousands of forensic investigations. Ms. Stoneman is a Certified Computer Examiner (CCE) through The International Society of Forensic Computer Examiners.

www.PacktPub.com

For support files and downloads related to your book, please visit www.PacktPub.com.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.



<https://www.packtpub.com/mapt>

Get the most in-demand software skills with Mapt. Mapt gives you full access to all Packt books and video courses, as well as industry-leading tools to help you plan your personal development and advance your career.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser

Customer Feedback

Thanks for purchasing this Packt book. At Packt, quality is at the heart of our editorial process. To help us improve, please leave us an honest review on this book's Amazon page at <https://www.amazon.com/dp/1787288684/>.

If you'd like to join our team of regular reviewers, you can e-mail us at customerreviews@packtpub.com. We award our regular reviewers with free eBooks and videos in exchange for their valuable feedback. Help us be relentless in improving our products!

Table of Contents

Preface	1
Chapter 1: Incident Response	7
The incident response process	8
The role of digital forensics	11
The incident response framework	12
The incident response charter	12
CSIRT	13
CSIRT core team	14
Technical support personnel	16
Organizational support personnel	17
External resources	19
The incident response plan	20
Incident classification	21
The incident response playbook	23
Escalation procedures	25
Maintaining the incident response capability	26
Summary	28
Chapter 2: Forensic Fundamentals	29
Legal aspects	29
Laws and regulations	30
Rules of evidence	31
Digital forensic fundamentals	32
A brief history	32
The digital forensic process	34
Identification	35
Preservation	35
Collection	36
Proper evidence handling	36
Chain of custody	37
Examination	40
Analysis	41
Presentation	41
Digital forensic lab	42
Physical security	42
Tools	43
Hardware	43

Software	46
Jump kit	52
Summary	54
Chapter 3: Network Evidence Collection	55
<hr/>	
Preparation	55
Network diagram	56
Configuration	57
Logs and log management	57
Network device evidence	59
Security information and event management system	61
Security onion	63
Packet capture	64
tcpdump	65
WinPcap and RawCap	68
Wireshark	70
Evidence collection	73
Summary	75
Chapter 4: Acquiring Host-Based Evidence	77
<hr/>	
Preparation	77
Evidence volatility	78
Evidence acquisition	78
Evidence collection procedures	80
Memory acquisition	81
Local acquisition	82
FTK Imager	82
Winpmem	85
Remote acquisition	88
Winpmem	88
F-Response	89
Virtual machines	98
Non-volatile data	99
Summary	100
Chapter 5: Understanding Forensic Imaging	101
<hr/>	
Overview of forensic imaging	101
Preparing a stage drive	104
Imaging	109
Dead imaging	109
Live imaging	120
Imaging with Linux	122

Summary	128
Chapter 6: Network Evidence Analysis	129
Analyzing packet captures	129
Command-line tools	130
Wireshark	131
Xplico and CapAnalysis	138
Xplico	138
CapAnalysis	142
Analyzing network log files	148
DNS blacklists	150
SIEM	152
ELK Stack	152
Summary	155
Chapter 7: Analyzing System Memory	157
Memory evidence overview	157
Memory analysis	158
Memory analysis methodology	158
SANS six-part methodology	159
Network connections methodology	160
Tools	160
Redline	160
Volatility	169
Installing Volatility	169
Identifying the image	170
pslist	171
psscan	172
pstree	173
DLLlist	174
Handles	174
svcscan	175
netscan and sockets	176
LDR modules	177
psxview	178
DllDump	179
memdump	181
procdump	183
Rekall	184
imageinfo	185
pslist	186
Event logs	186
Sockets	187
Malfind	187

Summary	189
Chapter 8: Analyzing System Storage	191
Forensic platforms	191
Autopsy	194
Installing Autopsy	194
Opening a case	194
Navigating Autopsy	201
Examining a Case	204
Web Artifacts	206
Email	209
Attached Devices	210
Deleted Files	212
Keyword Searches	213
Timeline Analysis	215
Registry analysis	219
Summary	224
Chapter 9: Forensic Reporting	225
Documentation overview	226
What to document	226
Types of documentation	227
Sources	229
Audience	229
Incident tracking	230
Fast incident response	231
Written reports	239
Executive summary	239
Incident report	239
Forensic report	242
Summary	246
Chapter 10: Malware Analysis	247
Malware overview	248
Malware analysis overview	250
Static analysis	250
Dynamic analysis	252
Analyzing malware	253
Static analysis	254
Pestudio	254
Remnux	258
Dynamic analysis	261
Process Explorer	262

Cuckoo sandbox	263
Summary	270
Chapter 11: Threat Intelligence	271
<hr/>	
Threat intelligence overview	271
Threat intelligence types	274
Threat intelligence methodology	275
Threat intelligence direction	277
Cyber kill chain	278
Diamond model	279
Threat intelligence sources	281
Internally developed sources	281
Commercial sourcing	282
Open source	282
Threat intelligence platforms	283
MISP threat sharing	284
Using threat intelligence	288
Proactive threat intelligence	289
Reactive threat intelligence	291
Autopsy	291
Redline	292
Yara and Loki	294
Summary	299
Index	301
<hr/>	

Digital Forensics and Incident Response

Biblioteka Główna
Akademii Sztuki Wojennej

26614/III (CB)



03-026614-000-0

Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with the preparatory activities associated of creating an incident response plan with creating digital forensics capabilities within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive analysis, and collecting network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom.

By the end of the book, you will have mastered forensic techniques and incident response, and you will have a solid foundation from which to increase your ability to investigate such incidents in your organization.

Things you will learn:

- Create and deploy incident response capabilities within your organization
- Build a solid foundation for acquiring and handling suitable evidence for later analysis
- Analyze collected evidence and determine the root cause of a security incident
- Learn to integrate digital forensic techniques and procedures into the overall incident response process
- Integrate threat intelligence in digital evidence analysis
- Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies

Packt
www.packtpub.com

₹999

Prices do not include local sales
Tax or VAT where applicable

FOR SALE IN INDIA ONLY

