Gerard Johansen

Digital Forensics and Incident Response

An intelligent way to respond to attacks

Packt›

Digital Forensics and Incident Response

An intelligent way to respond to attacks

Gerard Johansen

Packt>

BIRMINGHAM - MUMBAI

Digital Forensics and Incident Response

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

Reviewer
Nicole L. Stoneman

Acquisition Editor
Rahul Nair

Content Development Editor
Abhishek Jadhav

Technical Editor
Manish D Shanbhag

Production Coordinator
Aparna Bhagat

Copy Editor
Safis Editing

Project Coordinator
Judie Jose

Proofreader
Safis Editing

Indexer
Aishwarya Gangawane

Graphics
Kirk D'Penha

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

Digital Forensics and Incident Response

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

₹999

Packt›
www.packtpub.com

Prices do not include local sales
Tax or VAT where applicable

FOR SALE IN INDIA ONLY

ISBN 978-1-78728-868-3
54499
9 781787 288683