SpringerBriefs on Cyber Security Systems and Networks

The series aims to develop and disseminate an understanding of innovations, paradigms, techniques, and technologies in the contexts of cyber security systems and networks related research and studies. It publishes thorough and cohesive overviews of state-of-the-art topics in cyber security, as well as sophisticated techniques, original research presentations and in-depth case studies in cyber systems and networks. The series also provides a single point of coverage of advanced and timely emerging topics as well as a forum for core concepts that may not have reached a level of maturity to warrant a comprehensive textbook. It addresses security, privacy, availability, and dependability issues for cyber systems and networks, and welcomes emerging technologies, such as artificial intelligence, cloud computing, cyber physical systems, and big data analytics related to cyber security research. The mainly focuses on the following research topics:

Fundamentals and Theories

- Cryptography for cyber security
- Theories of cyber security
- Provable security

Cyber Systems and Networks

- Cyber systems security
- Network security
- Security services
- Social networks security and privacy
- Cyber attacks and defense
- Data-driven cyber security
- Trusted computing and systems

Applications and Others

- Hardware and device security
- Cyber application security
- Human and social aspects of cyber security

More information about this series at http://www.springer.com/series/15797

Chee Keong Ng · Lei Pan
Yang Xiang

Honeypot Frameworks and their Applications: A New Framework

Springer

Chee Keong Ng
School of Information
Deakin University
Burwood, Melbourne, VIC
Australia

Yang Xiang
Digital Research and Innovation Capability
Swinburne University of Technology
Hawthorn, Melbourne, VIC
Australia

Lei Pan
School of Information
Deakin University
Burwood, Melbourne, VIC
Australia

ISSN 2522-5561 ISSN 2522-557X (electronic)
SpringerBriefs on Cyber Security Systems and Networks
ISBN 978-981-10-7738-8 ISBN 978-981-10-7739-5 (eBook)
https://doi.org/10.1007/978-981-10-7739-5

Library of Congress Control Number: 2018938790

Printed on acid-free paper

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
part of Springer Nature
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

This book is dedicated to those who are interested to know more about honeypots. It does not matter whether you are an expert or novice, this book is for you.

Preface

Most people understand honeypots as systems sit in an isolated corner of the network waiting for attacker to discover and compromise them. This is often untrue, in fact, in some frameworks, honeypots have enjoyed the prime spot in an organisational network to lure potential hacker. As new instances of malware appear so rapidly that more spotlight has been placed in honeypot technology.

This book gives a detailed description of honeypots including their forms, purposes, natures and interaction. It also gives an in-depth introduction of different types of honeypot, their applications in monitoring and capturing of malware and adversary tactic to detect honeypot.

The main role of honeypot which effectively assists the researcher to derive solutions for the deadly malware attack has been outlined in the book. This book also gives rich information of other roles and uses of honeypot not only in the area of cyber and network security, but also in collecting proof for forensic investigation.

Finally, this book addresses the importance of honeypot as a learning tool for detecting future malware such as ransomware.

Burwood, Melbourne, Australia	Chee Keong Ng
Burwood, Melbourne, Australia	Lei Pan
Hawthorn, Melbourne, Australia	Yang Xiang

Acknowledgements

Thanks to Almighty God for enabling and helping me to complete this book.

I would like to first express my appreciation to my family, especially my wife, Xinying Liu, for her support and love. I would like to also express my most sincere gratitude to my supervisor, Prof. Xiang Yang, and Dr. Lei Pan for their wisdom and advice which is essential for the completion of this book.

Next, I would like to also express my token of appreciation to NSCLab, especially Dr. Jun Zhang for their moral support.

Lastly, I would like to thank Springer Publication for giving me this opportunity to spare my knowledge and finding in their book. I would also like to express my thanks to the editor, Dr. Xiaolan Yao, for her patient and assistance.

Contents