Review of the book

"Honeypots: A New Paradigm to Information Security"

by R. C. Joshi and Anjali Sardana

CRC Press, 2011

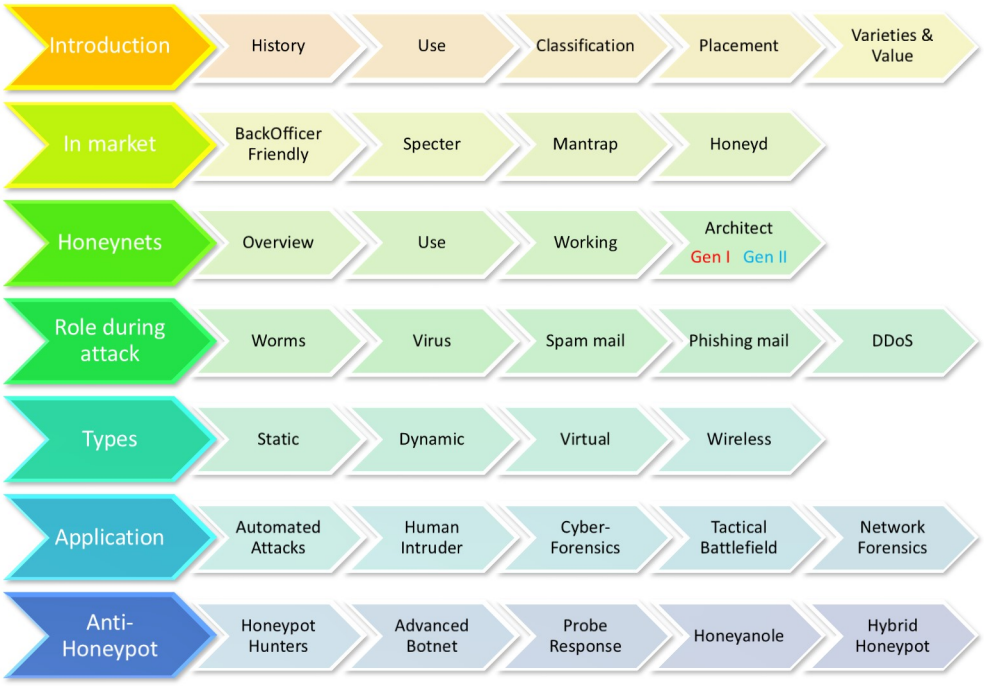
ISBN: 978-1-578-08708-2

Nishant Doshi
MEFGI, Gauridad Campus, India

1 Summary of the review

This book discusses about honeypot from history to present. The way authors added various case studies (including use of honeypot as savior) in chapters is admirable. The list of references for each chapter is also good way for the readers to easily locate the source of information. I suggest to add the further finding topic for each chapter in the future versions of books specially for researchers. The crisp intro and summary is also admirable as readers can get the bird eye view of chapters.

In addition, each chapter start with chapter outline and ends with chapter summary. This is useful for reader to get the insights of chapter like abstract and conclusion of paper. Also, in many chapters various tools were explained with step-by-step method. In the preface, the authors have nicely covered the objective, intended audience, organization of the book and pre-requisites. For simplicity, below figure depicts the overview of chapters.



It would be helpful if after each chapter, the authors put/mention further finding section that helps for researchers to work in this area.

For the researchers, this book gives the fundamentals understanding of the honeypot and its workings in the various environments. I will recommend this book to the UG students to strengthen their fundamentals on honeypots. For the PG student (and researchers too) to get the well depth understanding with further scope of improvements in the honeypots and its analysis.

2 Summary of the book

Chapter 1 This chapter start with history of honeypot and gives the generic honeypot model. The difference between firewall, intrusion detection system (IDS) and honeypot is clearly explained. Afterwards the classification of honeypots given based on different parameters like usage, interaction, etc. Then it leads to the placement of honeypots i.e. internal, external or DMZ. At last the key issues , risk and challenges were nicely discussed. Surely this chapter is the introduction for novice users to be familiarize with basics of the honeypot.

Chapter 2 After having familiarize with honeypots in previous chapter, this chapter discussed the four commercially available honeypots viz. BackOfficer Friendly, Specter, Mantrap and Honeyd. This chapter contains step-by-step introduction of each of honeypots with screen-shots of their user interface. Also, the authors have nicely explained the requirements of each of the honeypot in various situations.

Chapter 3 This chapter discusses about the today's and one of the most complex honeypot system called honeynets. It start with overview and justification of honeynets as complex system. Afterwards, it discusses the Gen-I honeypots. Then, the authors have discussed the issues in Gen-I honeypots. This can be helpful for researchers (and for attackers too) to work in this area. Afterwards, it discusses about the Gen-II honeynets that have incorporated the issues of Gen-I. At final, it discusses the risk management associated with honeynets and the sample systems of it.

Chapter 4 After getting depths of honeypot and forms of it in today's market, this chapter discuss about different attacks like virus, worm etc. and how honeypot plays role in it. It starts with different phases of attack and how honeypot can be helpful in each phase i.e. prevention, detection, response and research. Afterwards, it discusses the worms and how honeypot can be deployed to detect worms either in header or in payload. Then it lead to virus and the mails (spam and phishing) and finally DDoS attacks. In a nut shell, this chapter discusses the various attacks (that too is dangerous today) and how honeypot can be helpful to avoid this or make it less effective on the less users.

Chapter 5 This chapter discusses the form of honeypot in which honeypot system's location is fixed, also called as static honeypot. Compare to other systems (in upcoming chapters), the setup of static honeypot is simple. However, this system is more vulnerable to attacks as it fix to one location only. This chapter discusses the Japonica framework and its different layers. At last, it shows the use of this honeypot as deception system and furthers as deception Tool Kit model.

Chapter 6 As the previous chapter deals with static honeypot, this chapter discusses about virtual honeypot system. As it is evident that, we can bale to run one physical operating system (called guest OS), while many virtual OS within single machine (using VMWare). This leads to a more manageable system with cost efficient. The same phenomenon lead to the concept of virtual honeypot where it runs on virtual machine rather than physical machine. This chapter starts with concept of raw and virtual disks. The interesting part of this chapter is the detailed case study that is considered by the authors very well. I hope to see similar in-depth case studies in future books in each chapter.

Chapter 7 As the previous chapters deals with static type of honeypots (which requires constant care and look for the constant update), this chapter deals with dynamic honeypot in which once deployed, it takes care of itself with nearby environment and requirements easily. This chapter discusses the design and construction of dynamic honeypot system. At last it discusses the HoneyD as one of the dynamic honeypot system with its GUI. The benefits and issues in dynamic honeypot system were also nicely discussed.

Chapter 8 While the previous chapters deals with wired network based honeypot, this chapter deals with wireless network based honeypot. It starts with basics of WLAN and its basic concepts. Afterwards, the attacks in this type of network is also nicely covered. Then, the authors have explained the design of the wireless honeypot with its architecture. Finally, the limitation of wireless based honeypot were covered.

Chapter 9,11 As the previous chapters discusses about types of honeypot, this chapters discusses it use in the various application including automated attacks, network & cyber forensics and so on. As this chapter doesn't cover the in-depth analysis in each application, I suggest the reader to follow the references for the interested applications.

Chapter 10 The motive of this chapter is against the motive that were discussed in previous chapters. This chapter discusses the techniques that were used by researchers (and attacker too) to identify and removal of the detected honeypot. This chapter consists practical case studies to see and get the in-depth knowledge of honeypot removal.

3 Comments and Recommendations

I likes about this book is to considering various example scenarios and case studies in chapters. Also, in-depth discussion of some tools by which one can do such kind of analysis as it also handful for the students and the researchers. This book is the bridge for students to learn about what is security and how to prevent it using honeypot systems, thus from study to the research. One advancement in this book that I suggest is to add the further findings section in each chapter which specially used by researchers for motivation or guide the further scope in that field. As information security and thus the honeypots are in demand topic in today's world. the discussion of real time example scenario considered in this book is admirable.

On an average, this book gives the undergraduate students (of pre-final year), postgraduate students, researchers, scientists and so on to motivate and also to study further in the security in communication network and prevention using honeypots. Surely, I suggest this book as first hand book in cryptography for UG, PG and the researchers.

The reviewer is a faculty at MEFGI, India.