Preface

To best defend yourself and to defeat your enemies, you must first understand them: who they are, how they operate, and why. Throughout the ages, countless armies have used this strategy of studying and understanding their enemies in order to defeat them. Just as this strategy was applicable in the days of Julius Caesar, Jan III Sobieski, and Genghis Khan, it can also be applied today in the world of cyberspace. However, whereas enemies of the past may have brandished swords and cannons, today's cyberspace enemies attempt to compromise, steal, or damage information resources using computers and Internet Protocol (IP) packets as their battlefields and weapons.

We all know that computers, networks, software applications, and the Internet have introduced opportunities to the world that no one thought possible. However, as is true with any technology, these same opportunities also carry risks. Whether they are called blackhats, hackers, crackers, disgruntled employees, insiders, or just plain attackers, technology has given these individuals a means to attack almost any resource in the world. While the computer systems and networks we rely on provide us with amazing power, these same systems and networks are static targets: In order to communicate with the rest of the world they must virtually "stay in one spot," which is a critical vulnerability. Blackhats can launch attacks against these information systems whenever they want, however they want, from wherever they want. In many ways, they have the initiative. No

other technology has held such great potential for constructive purposes while at the same time giving attackers so much power to destroy that same potential. Thus, the Internet has created a global battlefield that spans not only governmental, military, and private enterprise sectors, but also the homes of millions of individual users.

Organizations, businesses, and individual computer owners spend millions of dollars each year to protect their computer resources against these attacks. Virus scanners, firewalls, intrusion detection systems (IDSs), encryption—all of these technologies and techniques are used to protect information systems against attacks. However, the bad guys still succeed, and their success is growing exponentially. One reason for this string of successes is that very few individuals or organizations have taken a step back to better understand who and what the nature of the threats are, how they operate, and why. Only when we are armed with this knowledge, can we better defend against and defeat our enemies.

This book explains the nature of some of these very real threats and gives you the tools and techniques to better learn who your enemies are, how they operate, and why they choose to do so. To do this, we will teach you about "honeynets," a relatively new security technology made up of networks of systems that are *designed* to be compromised. When attackers break into a honeynet, their every activity, their every keystroke, email, and toolkit is captured, allowing you to see step-by-step how they operate. By learning how to analyze the data honeynets collect, you can better understand who your enemies are and know what you need to do to protect your systems from them.

The first book to discuss honeynets was the first edition of *Know Your Enemy*, written by Honeynet Project members in 2001. This book introduced the concepts of honeynets, how they worked, and how to analyze the information they captured. Since then, radical improvements have been made, not just in honeynet technology, but in deployment concepts and how to analyze the information collected by honeynets. Thus, the second edition of *Know Your Enemy* discusses the advances made since 2001. This new edition covers the older honeynet technologies covered in the first edition—now considered first-generation technologies—in greater detail, offers more examples, and introduces new tools for deploying and maintaining honeynets. Even more exciting, this second edition

discusses new techniques and technologies never published before, including second-generation and distributed honeynets. Most of these new techniques have been tested and deployed by the Honeynet Project and Honeynet Research Alliance. The second edition also discusses data analysis in much greater detail, with entire chapters dedicated to Windows forensics, UNIX forensics, reverse engineering, and network forensics. All of this material is based on our experiences, with real-world examples to show you step-by-step all the issues involved.

Perhaps most exciting about the second edition is that each chapter is written by specific members of the Honeynet Project, Honeynet Research Alliance, and contributors—people who have developed and deployed the technologies the book discusses in the real world. These are people and organizations who have had their honeynets repeatedly attacked and have learned from their success and failures, and now hope to share their experience with you. We hope you find this book as exciting and fun as we have found our research to be.

FORMAT OF THE BOOK

The format of this book is very similar to our first edition and is broken down into three main parts:

- **Honeynets, Chapters 1–8:** In the first part, we discuss honeynets—what they are, their value, the different types, and how they work (in excruciating detail). We begin with the history of the Honeynet Project, then move onto what honeypots and honeynets are, their value, and the issues involved. We then discuss specific honeynet technologies (GenI and GenII) and move on to some more advanced deployments, such as virtual or distributed honeynets.
- **Analysis, Chapters 9–15:** In the second part, we discuss how to analyze the data honeynets collect, including network and disk forensics and data analysis. We attempt to go into as much detail as possible, using real data from a variety of different attacks we have captured.
- **Examples, Chapters 16–20:** In the third part, we cover what we have learned about common threats, using some examples of honeynets we have had compromised.

Finally, in Chapter 21, we finish the book up by discussing the future of this technology, and where it may be headed.

At the end of the book you will find several appendixes detailing configurations and data output from critical tools.

THE AUDIENCE OF THIS BOOK

Honeynets are used primarily for gathering information on threats. The information they collect has different value to different people, such as identifying insider threats, early warning and prediction, or intelligence gathering on specific new exploits, tools, or threats. This information can also shed light on the attackers themselves, revealing who is launching attacks, how they communicate, and what their motivations are. Thus, this book's target audience is security professionals—individuals who deal with attackers and have to protect their organizations on a daily basis.

Honeynets can capture and analyze information about attackers in both internal and external networks. Thus, in addition to security professionals, other organizations can benefit from this book. Security research organizations and universities can use the material in this book to conduct research on cyber threats using techniques that include content analysis or statistical analysis. Meanwhile, cyber attacks represent a serious threat against the critical information infrastructure of countries and governments, and cyber crime is a new threat law enforcement must deal with on a daily basis, with perpetrators being located all over the globe. Therefore, this book can also help government and law-enforcement organizations better understand and protect themselves against such threats by utilizing honeynets as a tool to identify, counter, and prosecute criminal activity. Military organizations will also find this book valuable, as cyber warfare has become a new, largely not understood, battleground, and honeynets can be deployed as a form of military intelligence. Finally, organizations and legal professionals will find Chapter 8 to be especially interesting, as it is one of the first definitive resources concerning the legal issues of honeynets, written by a member of the United States Department of Justice.

COMPANION CD-ROM

This book also comes with a companion CD-ROM, providing you with all the tools, materials, source code, and data captures discussed in the book. In addition, this CD provides the documentation, configuration files, and techniques for deploying honeynets, as well as the logs, network captures, and disk images of numerous attacks. Our goal is not just to educate you, but to provide you with the resources you need to gain hands-on experience.

COMPANION WEB SITE

The book also has a companion Web site (*http://www.honeynet.org/book*) whose purpose is to keep this material updated and to correct any discrepancies or mistakes identified in the book. For example, if any of the URLs mentioned in the book change, the book's Web site will provide you with updated links. In addition, you can visit the Web site to stay up-to-date with the latest in honeynet strategies.

CHAPTER REFERENCES

At the end of this book you will find a Resources and References section. This section will list, by chapter, all references made by that chapter, and where the reader can find additional information about topics discussed in this book. Examples include Web sites, white papers, and other books.

NETWORK DIAGRAMS

Throughout this book you'll also find network diagrams demonstrating the deployment of honeynets. To help you better understand all the technologies involved, when possible we use different images for different types of systems. Honeynets consist of two different systems: those that you want to be attacked and those you do not. All production systems are illustrated as simple black and white

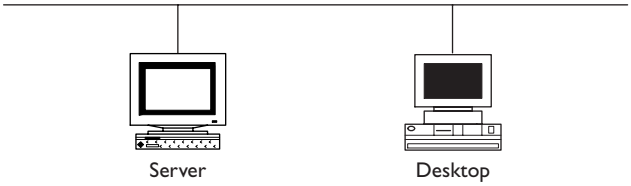

Figure A Two black and white production systems deployed on a network. These are systems you do not want to be attacked.

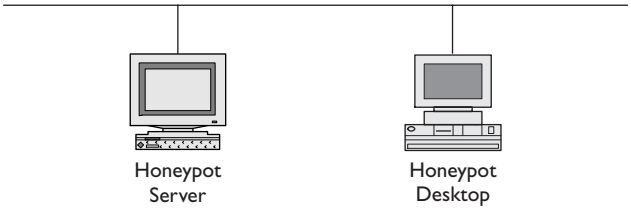

Figure B Two shaded honeypots deployed on a network. These are systems you do want to be attacked.

computer objects, as shown in Figure A. These are systems that you *do not* want to be attacked or compromised as they make up the internal architecture of a honeynet or are real-world production systems within an organization. Such systems include firewalls, intrusion detection sensors, and data collection systems.

Systems within honeynets that you *do* want to be attacked are illustrated throughout the book with gray shading going through the system, as shown in Figure B. These systems are referred to as "honeypots."

ABOUT THE AUTHORS

As noted earlier, this book was written by members of the Honeynet Project, Honeynet Research Alliance, and active contributors. Each chapter was written by the members with the greatest experience in that area. These individuals are security professionals dedicated to learning more about the blackhat community

and sharing the lessons they've learned. Each member brings unique skills and experiences to the table. For example, some members have extensive experience with Windows or UNIX forensics, others in reverse engineering, while still others have expertise in intrusion detection development, firewalls, network architecture, exploit analysis or in fields such as social psychology, statistics, foreign language translation, and profiling. The unique, multidisciplinary approach and expertise of these individuals combine to create an effective team, and we hope a very educational book. You will find the biographies of the authors involved in the creation of each chapter at the end of this book.

ACKNOWLEDGMENTS

The Honeynet Project, the Honeynet Research Alliance, and this book are the result of the hard work and numerous contributions of the security community. We would like to thank everyone who has helped and contributed to our research. Examples include people volunteering to translate our white papers, people contributing to the Scan of the Month challenges, and developers who have released or tested honeynet-related tools. Unfortunately, we cannot list you all by name, but we know who you are and appreciate your help. Without the community's support and input, our research would have never been possible. Also, we would like to thank the team at Addison-Wesley. Having to deal with one geek writing a book is bad enough. Having to publish for a whole team of dysfunctional geeks is worse. We are especially grateful to Jessica Goldstein, Elizabeth Ryan, Lynda D'Arcangelo, and Shannon Leuma. One last thanks to the security folks at UUnet; Chris, we could not have done it without you!