
PREFACE

It began as an innocent probe. A strange IP address was examining an unused service on my system. In this case, a computer based in Korea was attempting to connect to a rpc service on my computer. There is no reason why anyone would want to access this service, especially someone in Korea. Something was definitely up. Immediately following the probe, my Intrusion Detection System screamed an alert: An exploit had just been launched. My system was under assault! Seconds after the attack, an intruder broke into my computer, executed several commands, and took total control of the system. My computer had just been hacked! I was elated! I could not have been happier.

Welcome to the exciting world of honeypots, where we turn the tables on the bad guys. Most of the security books you read today cover a variety of concepts and technologies, but almost all of them are about keeping blackhats out. This book is different: It is about keeping the bad guys in—about building computers you *want* to be hacked. Traditionally, security has been purely defensive. There has been little an organization could do to take the initiative and challenge the bad guys. Honeypots change the rules. They are a technology that allows organizations to take the offensive.

Honeypots come in a variety of shapes and sizes—everything from a simple Windows system emulating a few services to an entire network of productions

systems waiting to be hacked. Honeypots also have a variety of values—everything from a burglar alarm that detects an intruder to a research tool that can be used to study the motives of the blackhat community. Honeypots are unique in that they are not a single tool that solves a specific problem. Instead, they are a highly flexible technology that can fulfill a variety of different roles. It is up to you how you want to use and deploy these technologies.

In this book, we explain what a honeypot is, how it works, and the different values this unique technology can have. We then go into detail on six different honeypot technologies. We explain one step at a time how these honeypot solutions work, discuss their advantages and disadvantages, and show you what a real attack looks like to each honeypot. Finally, we cover deployment and maintenance issues of honeypots. The goal of this book is not to just give you an understanding of honeypot concepts and architecture but to provide you with the skills and experience to deploy the best honeypot solutions for your environment. The examples in the back are based on real-world experiences, and almost all of the attacks discussed actually happened. You will see the blackhat community at their best, and some of them at their worst. Best of all, you will arm yourself with the skills and knowledge to track these attackers and learn about them on your own.

I have been using honeypots for many years and I find them absolutely fascinating. They are an exciting technology that not only teaches you a great deal about blackhats but also teaches you about yourself and security in general. I hope you enjoy this book as much as I have enjoyed writing and learning about honeypot technologies.

AUDIENCE

This book is intended for the security professional. Anyone involved in protecting or securing computer resources will find this resource valuable. It is the first publication dedicated to honeypot technologies, a tool that more and more computer security professionals will want to take advantage of once they understand its power and flexibility.

Due to honeypots' unique capabilities, other individuals and organizations will be extremely interested in this book. Military organizations can apply these technologies to Cyberwarfare. Universities and security research organizations will find tremendous value in the material concerning research honeypots. Intelligence organizations can apply this book to intelligence and counterintelligence activities. Members of law enforcement can use this material for capturing of criminal activities. Legal professionals will find Chapter 15 to be one of the first definitive resources concerning the legal issues of honeypots.

CD-ROM

A CD-ROM accompanies this book and contains additional information related to the topics in the book. It includes everything from whitepapers and source code to actual evaluation copies of software and data captures of real attacks. This will give you the hands-on opportunity to develop your skills with honeypot technologies.

WEB SITE

This book has a Web site dedicated to it. The purpose of the Web site is to keep this material updated. If any discrepancies or mistakes are found in the book, the Web site will have updates and corrections. For example, if any of the URLs in the book have been changed or removed, the Web site will provide the updated links. Also, new technologies are always being developed and deployed. You should visit the Web site to stay current with the latest in honeypot technologies.

<http://www.tracking-hackers.com/book/>

REFERENCES

Each chapter ends with a references section. The purpose is to provide you with resources to gain additional information about topics discussed in the book. Examples of references include Web sites that focus on securing operating systems and books that specialize in forensic analysis.

NETWORK DIAGRAMS

This book contains network diagrams demonstrating the deployment of honeypots. These diagrams show both production systems and honeypots deployed together within a networked environment. All production systems and honeypots are standardized, so you can easily tell them apart. All production systems are simple black-and-white computer objects, as in Figure A.

In contrast, all honeypots can easily be identified by shading and the lines going through the system, as in Figure B.

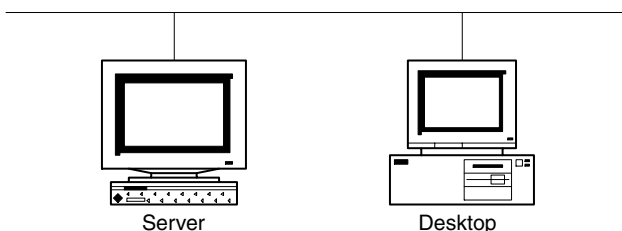


Figure A Two production systems deployed on a network

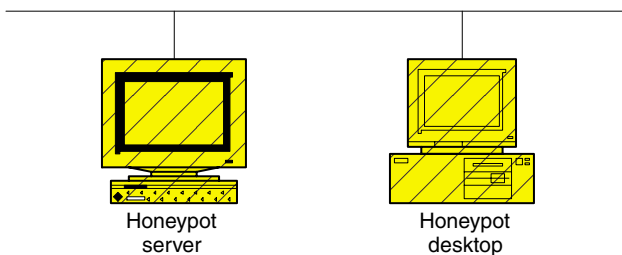


Figure B Two honeypots deployed on a network

ABOUT THE AUTHOR

Lance Spitzner is a geek who constantly plays with computers, especially network security. He loves security because it is a constantly changing environment. His love for tactics first began in the U.S. Army, where he served both as an enlisted

infantryman in the National Guard and as an armor officer in the Rapid Deployment Force. Following the Army he received his graduate degree and became involved in the world of information security. Now he fights the enemy with IPv4 packets instead of 120mm SABOT rounds.

His passion is researching honeypot technologies and using them to learn more about the bad guys. He is also actively involved with the security community. He is founder of the HoneyNet Project, moderator of the honeypot mail list, coauthor of *Know Your Enemy*, and author of several whitepapers. He has also spoken at various conferences and organizations, including Blackhat, SANS, CanSecWest, the Pentagon, the FBI Academy, West Point, National Security Agency, and Navy War College. He is a senior security architect for Sun Microsystems Inc.

ACKNOWLEDGMENTS

You could say that I did not really write this book. What I did was put together a great many concepts and technologies that I have been fortunate enough to learn from other people. Without their patience and help, not only this book but my career and education would not have been possible.

My sincere thanks go to the following.

The people who took the time to teach me when I was a neophyte. Kevin Figiel, you were priceless. You explained to me what Unix and a network are. I'll never forget my first day at work when you sat down and explained to me my first network diagram. The entire New Logic team, including Carlos Talbot, Jeff Vosburg, Corey Borin, and Robert Thomas, took the considerable time and effort to explain to me what Unix is all about and introduce me to the world of information security.

The folks at SANS, who have been big supporters since day one. I'll never forget how excited I was to make my first presentation on honeypots and tracking hackers. Stephen Northcut gave me my first chance to become involved with SANS. Alan Paller has been a committed supporter of honeypots and the HoneyNet Project. I would like to thank John Green, who has helped with both the Forensic

Challenge and HoneyNet Research Alliance. And finally, to the true boss at SANS, Zoe, the SANS goddess: Thank you so much for taking care of all of us.

Two gentlemen who were extremely influential in guiding me in the ways of computer security: Dan Farmer and Brad Powell. They are serious professionals from whom I have learned a great deal, including the Zen of security.

Marcus Ranum, one of the few people who continually develops crazier ideas than even I do. Your dedication to information security and innovative concepts is truly an inspiration.

The gents of SecurityFocus.com, to whom I owe more than a beer. Alfred Huger was one of the very first people to publish my whitepapers and support me in my work on honeypots. Other members, Elias Levy, Hal Flynn, and Ryan Russell, helped me in researching, understanding, and deploying honeypot technologies. I would also like to thank Elias for his commitment to the HoneyNet Project as one of our directors.

The men of Foundstone, one of the very first supporters of the HoneyNet Project and my research into honeypot technologies. Saumil, you are the “yaar”! Thanks to J. D. Glazer, Kevin Mandia, and Stuart McClure for their support, and to George Kurtz, the first director for the HoneyNet Project. Dave Wreski and the folks at linuxsecurity.com have been big supporters of honeypot technologies, the Forensic Challenge, and the HoneyNet Project.

Rob McMilan, Glen Sharlun, and other members of the Navy Postgraduate Program. This organization was one of the first to actively work with the HoneyNet Project on honeypot technologies. They opened my eyes to all the different possibilities of honeypots.

Richard Salgado and members of the Department of Justice. They have repeatedly gone out of their way to help the Project identify any legal issues with HoneyNet technologies.

The wonder weenies of the HoneyNet Project. Specifically Jeff Stutzman and Max Kilger, who can do more damage with numbers and data sets than anyone else I

know. David Dittrich, the most detail oriented person I know (in other words, anal). Your expertise in forensics and DoS attacks has been crucial to my understanding of honeypots and threats. David was also a major contributor to the chapter on honeypot legal issues. Marty Roesch, the network pig himself. Snort has been absolutely critical to the history of honeypots. Without it, we would know far less about the blackhat community. Dragos Ruiu and those ever-sexy black leather pants. Frank Heidt, one of the few people I know who is more intense than I am when dealing with security technologies. K2, vacuum, and rain forest puppy. I'm not sure what I admire more—their dedicated professionalism or their cool handles. Michael Clark, one of the first proponents of virtual Honeynets. Jed Hail, creator of Hogwash, one of the first GenII technologies for data control. Eric Cole and Ed Skoudis, SANS wonder twins. You two bums have been a huge help since I first began in the security field. Fyodor, Mr. Nmap himself. Robin Wakefield, one of the few people crazy enough to support the Honeynet Project from the beginning. Chris Brenton, one of the very first members of the Honeynet Project. Anne Tennholder, a huge supporter of the honeypots. Ofir Arkin—no man knows ICMP like Ofir. Max Vision, the master at decoding worms and exploits. Dug Song, the most frightening man in the world when it comes to coding layer two attacks. And the rest of the Honeynet Project: Dudes, without your skills, experience, and input, our research into honeypot technologies would have never been possible.

Bruce Schneier and Jennifer Grannick, two individuals crazy enough to support the Honeynet on the Board of Directors. Bruce, your insight to the potential of honeypots is setting the future for honeypot technologies. Jennifer, you have been an incredible leader in the legal issues of honeypots. Jennifer was also a major contributor to the chapter on honeypot legal issues.

The Honeynet Research Alliance, organizations daft enough to become involved in honeypot research. The South Florida Honeynet Project is led by Richard La Bella. Your devotion and motivation to Honeynet research is an inspiration to the security community. To the teams in Greece, India, and Mexico: It's great to see honeypots and community support have a global perspective. And to all the other members of the Alliance, thanks for your unique ideas and support.

My fellow geeks at the GESS Security Team at Sun Microsystems. With your support, guidance, and wisdom, I have a job I love and continually learn from. To John Totah, the most paranoid and finest security professional I know. To Donna, the kernel hacker goddess. Rob, Joel, and Robin, you have been guiding me from the start. To Brad Powell, the reason I joined Sun. To Ed, my boss, for putting up with all my crazy antics over the past three years. And to the rest of the team—hang in there, guys!

My fellow publisher and editors. You have always been and continue to be there for me. Karen Gettman, Emily Frey, Tracy Russ, Gioconda Mateu, and Mary Cotillo, and the rest of the A-W team, thanks for all the support. (I promise not to ask for too many copies of the book.) To Laurie McGuire, who was tasked with the grueling job of going through each chapter of the book and cleaning up the mess I created: I learned a great deal from you on how to write in a clean and concise manner. Char Sample, Richard Bejtlich, Sean R. Brown, Michael Clark, Marcus Leech, and Marcus Ranum—thanks for taking the time to review the book, find all my bone-headed mistakes, and make great suggestions for improving it!

Those folks I forgot to mention by name. You may have sent me an e-mail, posted on a mail list, or published a whitepaper on a Web site. Your contributions have helped me greatly.

Finally, my family. My parents were always there for me. Without their support and guidance—not to mention their babysitting skills—this book would have never been written. Thanks also to Ciocia, Busia, Grandpa, and the rest of my family. Most importantly, I would like to thank my wonderful wife, Ania, and our son, Adam. Without Ania's patience and support, I never would have been able to write this book. I would like to thank Adam for all of his unique input when he was at the keyboard helping me write this book. His keystroke combinations still defy me to this day (not bad for a 16-month-old!).