Foreword

We've all heard the phrase "knowledge will set you free." When it comes to real-world network security, I can think of no other phrase with which security professionals must arm themselves. Whether you are brand new to network intrusion detection, an incident responder, or a long-time network security veteran, you must always boil any situation down to its basic facts.

The book you are about to read will arm you with the knowledge you need to defend your network from attackers, both the obvious and the not so obvious. Unlike other computer security books that focus on catching the "hack of the week," this book will equip you with the skills needed to perform in-depth analysis of new and emerging threats. This book discusses many different approaches to network security. It also describes how to communicate and in some cases justify security monitoring efforts. This is important because many organizations may not readily appreciate the need for monitoring—until it is too late.

Frequently I run into security "professionals" who rely on "cookbook" methodologies or their favorite tools. Too often, these people do not have a broad understanding of how networks really work and are not effective in increasing their network's defensive posture or communicating with the network administrators. Although there is no substitute for actual system and network administration experience, by reading this book you will undoubtedly come away knowing more relevant information than when you started. In many large organizations, to gain the respect of the system or network administrators, you need to be able to converse at their level—even if it is way above or below your expertise.

The amount of plain talk in this book struck me as amazing. Firewalls can fail! Intrusion detection systems can be bypassed! Network monitors can be overloaded! We don't normally hear these messages from our vendors, nor do we hear it from our security administrators. Neither the vendor nor the administrator would be very successful if they focused on all the things that could go wrong. Unfortunately, this creates many false perceptions in the minds of managers and users.

You will enjoy the many examples in this book that show how a network is compromised and how it could have been prevented with some extra monitoring. Another dirty little secret that many security professionals don't speak much about is that our own tools are sometimes the most insecure portion of a network. You may be quite surprised to find out that the server set up to do sniffing or monitoring may be the gateway into the very network you are defending. You will learn ways to mitigate that threat too.

I strongly urge you to try using the tools described throughout this book while you are reading it. All of the tools are available for FreeBSD, Linux, and, in many cases, Windows. Although it may take longer to read the book, learning by using is more effective than skimming the command-line syntax.

If you are new to network security, don't put this book back on the shelf! This is a great book for beginners. I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial intrusion detection system, you may be asking, "What's next?" If so, this book is for you.

Some people have been performing network security monitoring for a very long time, and this book reviews that history. It will expose you to many other forms of monitoring that are not pure intrusion detection. The information about how you can use various tools to enhance your network security monitoring activities is an excellent resource all on its own.

I wish you the best of luck monitoring and defending your network!

Ron Gula
CTO and Founder of Tenable Network Security
Original author of the Dragon Intrusion Detection System