Foreword

When Syngress proposed Ethereal as the first book in my Open Source Security series, my first thought was "a whole book on Ethereal? Isn't it just a sniffer?" At the time, I didn't realize the scope of this program.

However, as we began developing the chapters, I saw exactly why Ethereal warranted an entire book. It has a tremendous number of useful features and included tools that most people never explore because it is so simple to use for day-to-day sniffing. Along these lines, chapter 6 (Other Programs Packaged with Ethereal) brings up less-often highlighted tools like *mergecap*, which many an IDS analyst or network forensics expert has used to read packet data from multiple sources and write that data out in the format of their choice. I recently spoke to an IDS expert who had never used *text2pcap*, (another tool covered by chapter 6) that he and I both found immensely useful in creating pcap packet captures from text-based hex-dumps. Chapter 7 (Integrating Ethereal with other Sniffers) offers an excellent treatment on how to interoperate Ethereal with a multitude of other free and commercial sniffers. Chapter 9's (Developing Ethereal) coverage of how to expand and build on Ethereal will prove useful for anyone who manages to find a protocol for which it doesn't yet have specific decoding functionality. And, I loved that chapter 5 (Filters) describes an undocumented feature in Ethereal so effectively and completely.

Most of all, I found chapter 8 (Real World Packet Captures) the most exciting. It demonstrates how to use Ethereal to dissect and understand attacks, allowing you to follow along by using Ethereal on the packet captures included on the accompanying CD-ROM. While the SQL Slammer and Ramen worm hands-on material was very interesting, I especially enjoyed following the Code Red analysis.

What comes out of reading these chapters is the realization that Ethereal is no run-of-the-mill freeware network sniffer. Ethereal offers more protocol

decoding and reassembly than any free sniffer out there and ranks pretty well among the commercial tools. We've all used tools like tcpdump or windump to examine individual packets (and always will), but Ethereal makes it easier to make sense of a stream of ongoing network communications. Ethereal not only makes network troubleshooting work far easier, but also aids greatly in network forensics, the art of finding and examining an attack, by giving a better "big picture" view. Finally, when you're trying to find, isolate, and understand anomalous traffic, its expandable-tree view of your network traffic is invaluable.

I hope that you'll find this book just as invaluable. Ethereal has the ability to be a simple, single-purpose tool that you use without thinking about when you need to look at packets, or it can be the backbone of your security toolkit. This book gives you the information you need to take Ethereal to whatever level of performance you want.

—Jay Beale