Foreword v 1.5

For the first edition of this book, the other authors and I had one thing in common: we all had something we wish we could have done differently in our chapters. We either made a mistake, or didn't explain something as well as we'd like, or forgot to cover something, or wish we had time to write one more bit of code. Like any project, the time eventually comes to cut the cord, and let it go.

Having a second chance to do this book again gives us the opportunity to change all those things we noticed from the moment the first book was printed. A good portion of those were due to the messages from readers that said, "you should have done this differently…". A great majority of the time, they were absolutely right. In the second edition of *Hack Proofing Your Network*, I've tried to incorporate as many of those suggestions as I could.

When *Hack Proofing Your Network* was first published, there were very few books on the market that taught penetration techniques outright. This book was the first of this genre for my publisher, Syngress Publishing. They were a little nervous. They weren't sure that teaching hacking techniques was such a great idea. (Other publishers must have been terrified. When I spoke to some of them about a "hacking book," they didn't even want to see an outline. "No hacking books." Of course, some of them now have books of their own in the genre.)

Consequently, Syngress felt that if we were to write *Hack Proofing Your Network,* the book should have coverage of defensive measures for everything. OK, I could do that. I've got nothing against defensive measures mind you, I've been using them for years. Some of my best friends are defensive measures. It just wasn't what I had in mind for this book. So, the first edition had a number of "defense" sections, which weren't as well done as they might have been, and generally made the flow awkward.

Well, some things have changed since the first edition of this book. For example, *Hack Proofing* is now a large series of books, not just a single title. As of this writing, these include:

Hack Proofing Your E-commerce Site (ISBN: 1-928994-27-X)

Hack Proofing Your Web Applications (ISBN: 1-928994-31-8)

Hack Proofing Sun Solaris 8 (ISBN: 1-928994-44-X)

Hack Proofing Linux (ISBN: 1-928994-34-2)

Hack Proofing Windows 2000 Server (ISBN: 1-931836-49-3)

Hack Proofing Your Wireless Network (ISBN: 1-928994-59-8)

Hack Proofing ColdFusion 5.0 (ISBN: 1-928994-77-6)

And there are more to come. These titles have at least one common feature: they are defense-oriented. That means that the authors of this book didn't have to worry about tacking on defense pieces this time around. Not that we didn't include *any*, but they were used only when they fit. (And just to prove that we don't have anything against the defense, many of us also did portions of the defense-oriented *Hack Proofing* books.)

This is Foreword version 1.5. This book has had an incremental upgrade (well, closer to an overhaul, but you get the idea.) However, Mudge's words still apply, so you'll find them next. Consider this to be a changelog of sorts. Allow me to cover some of the other new and improved changes to this edition. We're got several entirely new sections, including:

- Hardware hacking
- Tunneling
- IDS evasion
- Format string attacks

Again, this illustrates some of the nice things about being able to bring a book up to date; just after the first edition was published, format string exploits became public knowledge. We had no coverage of these in the first edition, as the exploit techniques weren't known.

Every other chapter has been brought up to date, retooled for an attack focus, tightened up, and generally improved. There are an infinite number of ways you can order these subjects, but some readers suggested that I should have organized the chapters from the first edition into a one-exploit-type-per-chapter order. Well, that sounded like a good idea, so you'll see that format in this book. There are still a couple of theory chapters at the front end, but following those "introductory" chapters, we launch right into the meat of how to accomplish each attack type. Finally, for the grand finale, we close the book with a quick chapter about reporting the holes you find (don't forget to tell all of us about it).

One major change in focus for this edition is that we've quit trying to explain ourselves. A great deal of time and effort was spent in the first edition trying to explain

why knowing "how to hack" was a good idea... *why* people use the word "hacker" at different times… and *why* reverse engineering should be a basic human right.

As it turns out, most of the people who bought the book already agreed that the information we presented should be available (or they at least wanted to have a look). And the people who didn't agree with me…well, they still didn't agree with me after reading the book, *even after reading my reasons*! Truthfully, I was appalled I wasn't changing anyone's mind with my careful arguments. If only someone had told me that I couldn't please all of the people all of the time.

So this time around, people who like what we do don't have to read why we do it, and people who don't can do… whatever they do. In case you're wondering, yes, we do use the word *hacker* to mean someone who breaks into computers without permission. However, it is not used solely in that context. It is also used in a variety of "subjective" definitions. You, as an educated reader and security professional, will just have to figure out from context which definition is meant, just like real life. If you read the rest of this book, you'll find that we even use the term in a way that includes *you*.

In case you're wondering exactly what was in the first edition that isn't here anymore, you can find out. Check out the Syngress Solutions site at **www.syngress.com/solutions** and activate your Solutions membership. In addition to the electronic version of the first and second editions of the book, you will find a feature where you can e-mail questions for me to answer about the book. And if that isn't enough, over the course of the next year you'll see periodic updates to the book in the form of whitepapers. It's just one more way for us to cover the new stuff that didn't exist until after the book came out. The Solutions site is your resource—use it. It'll make me happy too, I love hearing from readers.

I hope you enjoy the book.

—Ryan Russell