Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network

Table of Contents:

I Setting the Stage

II Understanding the Terrain

III Tools

IV Platforms and Security

V Beginning at Ground Zero

VI The Remote Attack

VII The Law

VIII Appendixes

Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network

Dedication

This book is dedicated to Michelle, whose presence has rendered me a prince among men.

Acknowledgments

My acknowledgments are brief. First, I would like to acknowledge the folks at Sams, particularly Randi Roger, Scott Meyers, Mark Taber, Blake Hall, Eric Murray, Bob Correll, and Kate Shoup. Without them, my work would resemble a tangled, horrible mess. They are an awesome editing team and their expertise is truly extraordinary.

Next, I extend my deepest gratitude to Michael Michaleczko, and Ron and Stacie Latreille. These individuals offered critical support, without which this book could not have been written.

Also, I would like to recognize the significant contribution made by John David Sale, a network security specialist located in Van Nuys, California. His input was invaluable. A similar thanks is also extended to Peter Benson, an Internet and EDI Consultant in Santa Monica, California (who, incidentally, is the current chairman of ASC X12E). Peter's patience was (and is) difficult to fathom. Moreover, I forward a special acknowledgment to David Pennells and his merry band of programmers. Those cats run the most robust and reliable wire in the southwestern United States.

About the Author

The author describes himself as a "UNIX propeller head" and is a dedicated advocate of the Perl programming language, Linux, and FreeBSD.

After spending four years as a system administrator for two California health-care firms, the author started his own security-consulting business. Currently, he specializes in testing the security of various networking platforms (breaking into computer networks and subsequently revealing what holes lead to the unauthorized entry) including but not limited to Novell NetWare, Microsoft Windows NT, SunOS, Solaris, Linux, and Microsoft Windows 95. His most recent assignment was to secure a wide area network that spans from Los Angeles to Montreal.

The author now lives quietly in southern California with a Sun SPARCStation, an IBM RS/6000, two Pentiums, a Macintosh, various remnants of a MicroVAX, and his wife.

In the late 1980s, the author was convicted of a series of financial crimes after developing a technique to circumvent bank security in Automatic Teller Machine systems. He therefore prefers to remain anonymous.

Tell Us What You Think!

As a reader, you are the most important critic and commentator of our books. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way. You can help us make strong books that meet your needs and give you the computer guidance you require.

Do you have access to the World Wide Web? Then check out our site at http://www.mcp.com.

NOTE: If you have a technical question about this book, call the technical support line at 317-581-3833 or send e-mail to suppor@mcp.com.

As the team leader of the group that created this book, I welcome your comments. You can fax, e-mail, or write me directly to let me know what you did or didn't like about this book--as well as what we can do to make our books stronger. Here's the information:

FAX: 317-581-4669

E-mail:

Mark Taber
newtech_mgr@sams.mcp.com

Mail:

Mark Taber
Comments Department
Sams Publishing
201 W. 103rd Street
Indianapolis, IN 46290

Introduction

I want to write a few words about this book and how it should be used. This book is not strictly an instructional, or "How To" book. Its purpose is to get you started on a solid education in Internet security. As such, it is probably constructed differently from any computer book you have ever read.

Although this book cannot teach you everything you need to know, the references contained within this book can. Therefore, if you know very little about Internet security, you will want to maximize the value of this book by adhering to the following procedure:

Each chapter (except early ones that set the stage) contains intermittent references that might point to white papers, technical reports, or other sources of solid, reliable information of substance (pertaining to the topic at hand). Those references appear in boxes labeled *XREF.* As you encounter each source, stop for a moment to retrieve that source from the Net. After you retrieve the source, read it, then continue reading the book. Throughout the book, perform this operation whenever and wherever applicable. If you do so, you will finish with a very solid basic education on Internet security.

I have constructed this book in this manner because Internet security is not a static field; it changes rapidly. Nonetheless, there are certain basics that every person interested in security must have. Those basics are not contained (in their entirety) in any one book (perhaps not even in dozens of them). The information is located on the Internet in the form of documents written by authorities on the subject. These are the people who either designed and developed the Internet or have designed and developed its security features. The body of their work is vast, but each paper or technical report is, at most, 40 pages in length (most are fewer than 10).

Those readers who want only a casual education in Internet security may read the book without ever retrieving a single document from the Internet. But if you are searching for something more, something *deeper*, you can obtain it by adhering to this procedure.

If you choose to use the book as a reference tool in the manner I have described, there are certain conventions that you need to know. If the resource you have been directed to is a tool, consider downloading it even if it is not for your platform. With a proper archive tool (like Winzip), you can extract the documents that accompany the distribution of that tool. Such documents often contain extremely valuable information. For example, the now famous scanner named *SATAN* (made expressly for UNIX) contains security tutorials in HTML. These do not require that you have UNIX (in fact, all they require is a browser). Likewise, many other tools contain documents in PDF, TXT, DOC, PS, and other formats that are readable on any platform.

TIP: SATAN is a special case. Some of the tutorials are in HTML but have `*.PL` extensions. These extensions are used to signify documents that are written in Perl. If you do not have Perl installed, convert these documents to raw HTML. To do so, open them in a text editor and replace the first line (`<< HTML`) with `<HTML>`. Then rename the file with either an `*.HTM` or an `*.HTML` extension. From that point on, your browser will load the pages perfectly.

Also, note that many of the Internet documents referenced in this book are available in PostScript form only. PostScript is a wonderful interpreted language that draws graphics and text. It is used primarily in technical fields. To view some of these documents, therefore, you will require a PostScript reader (or interpreter). If you do not already have Adobe Illustrator or some other proprietary PostScript package, there are two leading utilities:

- Rops
- Ghostscript/Ghostview

Both are freely available for download on the Internet. Rops is available here:

- `ftp://ftp.winsite.com/pub/pc/winnt/txtutil/rops3244.zip`

Ghostscript and Ghostview are available here:

- `ftp://ftp.cs.wisc.edu/ghost/aladdin/gs353w32.zip`
- `http://www.cs.wisc.edu/%7Eghost/gsview/index.html`

I should point out that Rops is shareware, while Ghostscript and Ghostview (hereafter, *the GS utilities*) are free. The chief differences between these two distributions are that Rops is smaller, easier to configure, and faster. In fact, it is probably one of the best shareware products I have ever seen; it is incredibly small for the job that it does and requires minimal memory resources. It was coded by Roger Willcocks, a software engineer in London, England.

In contrast, the GS utilities are slower, but support many more fonts and other subtle intricacies you will likely encounter in PostScript documents produced on disparate platforms. In other words, on documents that Rops fails to decode, the GS utilities will probably still work. The GS utilities also have more tolerance for faults within a PostScript document. If you have never used a PostScript interpreter, there are certain situations you may encounter that seem confusing. One such situation is where the interpreter cannot find evidence of page numbering. If you encounter this problem, you will only be able to move forward in the document (you will not be able to go back to page 1 after you have progressed to page 2). In such instances, it's best to print the document.

To avoid this problem, I have purposefully (and by hand) searched out alternate formats. That is, for each PostScript document I encountered, I tried to find the identical paper in PDF, TXT, DOC, WPG, or HTML. In some cases, I'm afraid, I could not find the document in any other form (this was especially so with early classic papers on Internet security). In cases where I did successfully find another format, I have pointed you there instead of to the PostScript version. I did this because the majority of PC users (with the exception of Mac users) do not routinely have PostScript facilities on their machines.

Next I need to say several things about the hyperlinks in this book. Each one was tested by hand. In certain instances, I have offered links overseas to papers that are also available here in the United States. This is because I tried to pick the most reliable links possible. By *reliable links*, I mean the links most easily retrieved in the shortest time possible. Although you wouldn't think so, some overseas links are much faster. Also, in some instances, I could only find a verified link to a document overseas (*verified links* means that when I tested the link, the requested item actually existed at the URL in question). To provide you with maximum value, I have attempted to reduce the incidences of `Object Not Found` to practically nil. Naturally, however, your mileage may vary. Sites often change their structure, so expect a few links to be no longer valid (even though most were checked just a month or two before the book's printing.)

Also, many hyperlink paths are expressed in their totality, meaning that wherever possible, I have extracted the *total* address of an object and not simply the server on which it resides. In reference to downloadable files (tools, usually), these links will not bring you to a page. Instead, they will initiate a download session to your machine, bringing the file directly to you. This will save you time, but might first be confusing to less experienced users. Don't be surprised when a dialog box appears, asking you to save a file.

Wherever I specify what language a tool or software program was written in, pay careful attention. Many tools mentioned require either a compiler or an interpreter before they can be built and used. If you do not currently have the language or interpreter necessary (or if your platform is different from that for which the tool was designed), re-examine the reference. Unless it seems that the distribution contains documents that are of value to you, you should probably refrain from downloading it. Moreover, many utilities come in source code form only. Although I have examined much of the source code myself, I cannot vouch for each and every line of it. If you intend to download source code and compile it on your own architecture, be aware that neither I nor Sams can be responsible for trojans or other malicious code that may exist in these files. The majority of files referenced are actually from reliable sources and many are accompanied by digital signatures, PGP keys, or other co-signing assurances of authenticity and integrity. However, code that originated on cracker sites may or may not be clean. Use your judgment in these instances.

> **NOTE:** Special note to Windows and Mac users: if you have no idea what I am talking about, fear not. You will by the time you reach Chapter 6, "A Brief Primer on TCP/IP." I made every possible attempt to make this book easily read and understood for all users. I have taken great pains to explain many terms and procedures along the way. If you are already aware of the definitions, skip these passages. If you are not, read them carefully.

The majority of the sites referenced are easily viewed by anyone. There may be a few sites that use extensive table structures or maintain an all-graphic interface. Those with noncompliant browsers may not be able to view these sites. Nonetheless, there are very few such sites. Wherever possible, I have attempted to find alternate pages (that support non-table browsers) so almost all of the pages are viewable using any browser. However, I am not perfect; my efforts may fail in some cases. For this, I apologize.

In reference to sites mentioned that I deem "very good," a word of caution: This is my opinion only. I classify sites as "good" if they impart information that is technically sound or point you in many valuable directions. But simply because I say one site is good and say nothing about another does not mean the other site is bad. I have hand-picked every site here, and each offers good information on security. Those I single out as particularly good are so identified usually because the maintainer of that site has done an exemplary job of presenting the information.

With respect to hyperlinks, I will say this: At the end of Appendix A, "Where to Get More Information," I offer an uncommented, bare list of hyperlinks. This is the equivalent of a huge bookmark file. There is a purpose for this, which I discuss in detail within that Appendix, but I will briefly address that purpose now. That list (which will also appear on the CD-ROM) is provided for serious students of security. By loading that list into a personal robot (Clearweb is one good example), you can build a huge security library on your local machine. Such personal robots rake the pages on the list, retrieving whatever file types you specify. For companies that have adequate disk space and are looking to build a security library, this can be done automatically. Most robots will clone a remote site within a few minutes.

Be aware, however, that the majority of links offered lead to pages with many links themselves. Thus, if you are running such a robot, you'd better have adequate disk space for the output. Printed in their native form, all retrievable documents in that list (if retrieved with a robot that goes out one level for each link) would print a stack of paper approximately seven feet tall. I know this because I have done it. In Appendix A, I describe the procedure to do so. If you decide to retrieve and print written information and binaries from all the sites listed, you will have the majority of written security knowledge available on the Internet within two weeks. In organizations doing serious security research, this could have significant value, particularly if all documents are reformatted to a single file format (you could do special indexing and so forth).

Certain books or other documents have been referenced that are not available online. These documents are obtainable, however. In all cases, I have included as much information on them as possible. Sometimes, the ISBN or ISSN is included, and sometimes not. ISBNs were not always obtainable. In these instances (which are admittedly rare), I have included the Library of Congress catalog number or other, identifying features that may help you find the referenced material offline. Any sources that could not be traced down (either on the Net or elsewhere) were omitted from the book.

Moreover, I have made every possible effort to give credit to individuals who authored or otherwise communicated information that is of technical value. This includes postings in Usenet newsgroups, mailing lists, Web pages, and other mediums. In almost all cases (with the exception of the list of vendors that appears in Appendix B, "Security Consultants"), I have omitted the e-mail addresses of the parties. True, you can obtain those addresses by going to various sites, but I refrained from printing them within this book. I have made every effort to respect the privacy of these individuals.

The list of vendors that appears in Appendix B was not taken from the local telephone book. In March 1997, I issued a bulletin to several key security groups requesting that vendors place a listing in this book. The people (and companies) who replied are all qualified security vendors and consultants. These vendors and individuals provide security products and services every day. Many deal in products that have been evaluated for defense-level systems or other typically secure environments. They represent one small portion of the cream of the crop. If a vendor does not appear on this list, it does not mean that it is not qualified; it simply means that the vendor did not want to be listed in a book written by an anonymous author. Security people are naturally wary, and rightly so.

In closing, I have some final words of advice. Appendix C, "A Hidden Message," points to a block of encrypted text located on the CD-ROM. The encryption used was Pretty Good Privacy (PGP). When (or rather, if) you decrypt it, you will find a statement that reveals an element of the Internet that is not widely understood. However, within five years, that element will become more clear to even the average individual. There are several things that you need to know about that encrypted statement.

First, the encrypted text contains my opinion only. It is not the opinion of Sams.net. In fact, to ensure that Sams.net is not associated with that statement, I have taken the precaution of refusing to provide employees of Sams.net with the private passphrase. Therefore, they have absolutely no idea what the statement is. Equally, I assure you (as I have assured Sams.net) that the statement does not contain profanity or any other material that could be deemed unsuitable for readers of any age. It is a rather flat, matter-of-fact statement that warns of one facet of the Internet that everyone, including security specialists, have sorely missed. This facet is of extreme significance, not simply to Americans, but to all individuals from every nation. At its most basic, the statement is a prognostication.

Now for a little note on how to decrypt the statement. The statement itself is very likely uncrackable, because I have used the highest grade encryption possible. However, you can determine the passphrase through techniques once common to the spy trade. Contained in Appendix C are several lines of clear text consisting of a series of characters separated by semi-colons (semi-colons are the field separator character). After you identify the significance of these characters, you are presented with some interesting possibilities. After trying them all, you will eventually crack that statement (the significance of the clear text fields will reveal the passphrase). If you are clever, cracking the message is easier than it looks (certainly, those wild and crazy characters at NSA will have no problem, as long as the folks doing it are vintage and not kids; that is about the only clue I will give). The public key for the message is `root@netherworld.net`.

If you crack the message, you should forward it to all members of Congress. For them, a group largely uneducated about the Internet, the message within that encrypted text is of critical importance.

Good luck.

Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network

For information, address Angel722 Publishing, 1800 Engel Rd. 3rd Floor,
Lawrence, Kansas, 66044

This material is provided "as is" without any warranty of any kind.