hacker reviews

***Secrets of a Super Hacker* by The Knightmare**
Loompanics Unlimited
205 pages, $19.95
Review by Michael E. Marotta

"Third time's the charm." This is the third book on hacking from Loompanics and it is the best of the three. (M. Harry's *Computer Underground* is also a fine work.) The book has some hype, but overall *Secrets of a Super Hacker* presents a complete summary of what every hacker knows. And what every wannabe wants to know.

There was a time when hackers earned their power. Working alone, each one found neat stuff. When BBS's were invented, hackers could share, but sharing was based on exchange: to get something, you had to have something you found on your own. When Stoll and Hafner wrote about hacking they were careful to say enough to give body to their narratives. But not too much. They never gave out passwords. This book blows all of that away. It is the *Jurassic Park* of hacking.

In *Jurassic Park*, the mathematician who dies rambles on under morphine about how power corrupts. He notes that the karate master doesn't beat his wife because becoming a master entails mastering himself. But the JP, Inc. folk *bought* their technology wholesale. They didn't have to earn their power. So, it was in control of them. *Secrets of a Super Hacker* will deliver into anyone's hands for $20 what it took us 30 years to learn. The appendix includes rtm's list of common passwords - in case you want to be a hacker but don't know how to FTP. From shoulder surfing to tempest, from social engineering to dictionary attacks, it's all in here. He even covers dumpster diving. The best part is the lengthy section on getting data from damaged diskettes. And then imagine hacking a computer network by splicing your notebook computer into the light pen of a terminal!

The Knightmare maintains that as more and ever more people come online, there will always be opportunities for the hacker. Somewhere there is a username/password combination SMITH/SMITH. Somewhere there is a new manager open to the "dumb user" ploy. You just have to find them. What do you do then? Well, the hacker ethic says don't screw things up. But the hacker ethic also says to explore. The Knightmare says that once you are inside a computer, you can prove to yourself that you are really a hacker by changing its databases and not getting caught.

Secrets of a Super Hacker is very readable. Its colloquial American crams a lot of information into each sentence. It is a very dense narrative. The organization is commendable. The book is divided into three sections: Before Hack, During Hack, and After Hack. The book begins with The Basics (hardware, software, etc.) and The History of Hacking (*YIPL, TAP, 2600*). Subsequent chapters include: Researching the Hack, Passwords and Access Control, Social Engineering, Reverse Social Engineering, and What to Do When Inside.

Naturally, there is a chapter on How to Keep from Getting Caught. At 10 cents a page, you can't go wrong.

UNIX Security: A Practical Tutorial
By N. Derek Arnold, ITDC
McGraw-Hill, Inc.
ISBN 0-07-002560-6
Review by Simson L. Garfinkel

While there is suddenly a plethora of UNIX security books on the market, almost all of them are written from the point of view of the system operator, feverishly bent on keeping hackers out of his computer while not making life too terrible for the legitimate users. While these books make interesting reading, it takes a lot of work between-the-lines to get any useful info out of these tomes about breaking into UNIX systems.

Thankfully, such is not the case with Arnold's *UNIX Security*. This is a book aimed at the hacker community, with detailed, step-by-step instructions for finding and exploiting vulnerabilities on all kinds of UNIX systems. Although the book is filled with tips, most hackers will turn straight to Chapter 8, "Break-in Techniques." The advice is all sound: patience is a virtue (and necessary if you don't want to get caught); arrange for evidence that points at somebody else; search out log files and cover your tracks. In addition to good technical know-how, Arnold shares tips on social engineering as well.

The only confusing aside is Arnold's belief that hackers are hell-bent on getting sysops fired. To this end, he suggests sending insulting or harassing forged electronic mail, allegedly from the sysop, to the sysop's manager. What sensible hacker would do this? Besides being a great way to get caught, there are simply so many more rewarding things that a hacker can do once gaining superuser privileges. Sadly, Arnold's book is a bit shy in this department.

As an added jackpot, Arnold's book contains over 140 pages of program listings. While some of the programs are of limited utility, the hacker's pride and joy are the fairly sophisticated password cracking program, the UNIX computer virus for infecting a.out files, and a utility for groveling through /dev/kmem.

UNIX Security's heavy System V bias makes it of limited value for hacking into the university world, but makes it ideal for those interested in breaking into business. Perhaps his goal in publishing this information is to create more work for computer security professionals. (Arnold's company, ITDC, is a McGraw-Hill consulting firm which teaches courses in computer security; this book is largely taken from ITDC's course notes.) With *UNIX Security*, a good laptop with a cellular modem, and a few day's supply of batteries, a young aspiring hacker could go far.