Hacking: The Next Generation
Nitesh Dhanjani, Billy Rios & Brett Hardin
O’Reilly

Book review by Katina Michael, School of Information Systems and Technology, University of Wollongong, Australia
Phone: +61242213937; Fax: +61242214045; katina@uow.edu.au

Hacking: The Next Generation demonstrates just how hackers continue to exploit “back doors”. New ways of working and new ways of communicating have meant that the number of attack vectors continue to rise rapidly. This provides hackers with a greater number of opportunities to penetrate systems using blended approaches while organizations struggle to come up to speed with the latest technology developments and commensurate security capabilities. Dealing with anticipated threats is a lot harder than dealing with known threats.

Dhanjani, Rios and Hardin are skillful in their analysis of hacking in the next generation, providing coverage of classic traditional attacks, as well as emerging threats in the cloud, mobile devices, and social networking. Emphasis is placed on phishing attacks, targeted attacks versus opportunistic attacks, and the well-known but increasingly troublesome insider attacks. The threesome are especially equipped with security-related knowledge- Dhanjani now a senior manager at Ernst & Young was previously the senior director of Application Security and Assessments at Equifax, Rios is a security engineer with Microsoft, and Hardin a security research Lead with McAfee.

On June 6, LinkedIn, the largest professional social network was hacked and 6.5 million unique hashed passwords appeared on a Russian cybercrime forum. Within the first 24 hours, it was purported that more than 200,000 passwords had been cracked. And not long after that, dating agency eHarmony and music site Lastfm.com also discovered that passwords of a small fraction of its user base had been compromised. As individuals scramble to remember passwords for a diverse array of online applications, the possibility that anyone having access to the leaked passwords could penetrate personal accounts of other online applications was very high. This book does not shy away from dealing with potential security breaches of this magnitude, and demonstrates how hackers might go about orchestrating such an attack.

Beyond a doubt, all the technical know-how proliferating in the hacker community is cause for concern but the traditional art of social engineering is developing just as fast in complexity and methodological rigor, as shown in this book. Coercion, manipulation and influence are just some of the tools of persuasion used by hackers against employees of organizations. But even more brazen has been the efforts of hackers against executives who may have a wealth of strategic business knowledge but little in the way of street sense when it comes to technology and more specifically non-technical security attacks. In fact, most executives today feel overwhelmed by the amount of organizational communications (and spam) they receive and happily grant their personal assistants access to a number of collaborative applications, including web conferencing, email and social media.

Critical data is also being leaked outside the organization using non-traditional tools, meaning that perimeter-based defense models are just not effective. These data leaks, while difficult to quantify unless penetration testing is regularly conducted, cost organizations
significant losses annually. But it is the “unknown” component of these losses which is especially worrying to organizations whose business models dictate an agile workforce through mobile and cloud solutions, connectivity between stakeholders for relationship management, and similar extensions.

What you can expect from this book is to learn new things about hacking that you were not aware of. I personally tested some of the scenarios and cases described in this book with an executive who initially did not believe that these were realistic hacking techniques that hackers would perform but who soon admitted to their possibility and potentiality.

The book is armored with excellent freely available online reference sources, commands that can be literally typed into an operating system, including programming source code, and typical scenarios and role play dialogues, and many supporting illustrations. It is bound to make you think differently about hacking as you might understand it in the new threat landscape.