Foreword

Penetration testing is one of those odd jobs you typically hear little about—it is like a black art, and can come with not only smoke and mirrors but, for the pen tester, any number of trap doors and blind alleys. Bits and pieces of penetration testing have made it into the mainstream media, culminating in the classic hacker-fave film *Sneakers,* starring Robert Redford, Sidney Poitier, and a host of other stars. And while plenty seems to be written about hacking and gaining access to systems, there has been nothing written that really speaks to the art of penetration testing.

Like most other high tech jobs portrayed in the movies, pen testing is not as glamorous as most people think. Oh sure, there are exciting moments, such as when the first system belonging to the target is penetrated, but it is actually hard work. Comparatively, a typical intruder's job is easy.

A regular electronic intruder has to find only one hole into an organization's computers, but a pen tester has to find them all. This is not only somewhat tedious and even boring at times, it is very important. The intruder probably does not care about such things as accidentally damaging systems, or wiping log files to hide his presence. The pen tester is trying to keep from disrupting normal business, preserve records and logs, yet still trying to move about unnoticed. In other words, to be a pen tester you have to have not only all of the intruder techniques possible, but also understand system administration as well as corporate life in general. Not an easy task.

FOREWORD

Many people who are new to the wily world of penetration testing quickly realize that there are not just drudgery tasks such as mapping out entire corporate networks and finding multiple attack vectors instead of just one. They also come face to face with a dizzying spectrum of contracts, clauses, guarantees, periodic midstream debriefings with confused clients, and everything else normal contractors might encounter, plus dozens more that a normal IT contractor would never hope to encounter. Can you essentially plan a legalized live simulation of a crime against a target, with the vast majority of personnel at the target unaware you are performing a simulation?

Hard as it may seem, it can be one of the most rewarding jobs a geek can get. It is more than "playing criminal," it is playing the ultimate game of chess—a chess game where you get to try out every move. You just have to document your moves so you can recreate your steps if needed.

The problem with most career choices is that unless you can sit down and talk with someone in the business, you can never fully appreciate what that career is all about. In the world of plumbers, you can go to the library and find tons of self-help books, and you probably either know a plumber or at least have a relative or friend who knows one you could talk to. Not the case with penetration testing.

Until now. This book covers not just the glamorous aspects such as the intrusion act itself, but all of the pitfalls, contracts, clauses, and other gotchas that can occur. The authors have taken their years of trial and error, as well as experience, and documented a previously unknown black art.

Penetration testing is important. It gives a company a chance to make sure their systems are secure, their incident response policies are in place, and give them not only peace of mind but possible compliance with the increasing insurance and government regulations placed upon them (HIPAA leaps to mind). But there are not enough good pen testers out there. This book helps to at least give you a leg up. There is nothing more frustrating when trying something new than to encounter unforeseen obstacles you never expected. This book isn't magic—the obstacles do not go away. But after reading you are aware of them, and have even been given some choices to help you get around them quickly. Enjoy the book.

Mark Loveless, aka Simple Nomad
Senior Security Analyst, BindView RAZOR Team