



Foreword

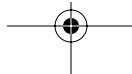
HONEYPOTS AND THE HONEYNET PROJECT



In warfare, information is power. The better you understand your enemy, the more able you are to defeat him. In the war against malicious hackers, network intruders, and the other blackhat denizens of cyberspace, the good guys have surprisingly little information. Most security professionals, even those designing security products, are ignorant of the tools, tactics, and motivations of the enemy. And this state of affairs is to the enemy's advantage.

The Honeynet Project was initiated to shine a light into this darkness. This team of researchers has built an entire computer network and completely wired it with sensors. Then it put the network up on the Internet, giving it a suitably enticing name and content, and recorded what happened. (The actual IP address is not published, and changes regularly.) Hackers' actions are recorded as they happen: how they try to break in, when they are successful, what they do when they succeed.

The results are fascinating. A random computer on the Internet is scanned dozens of times a day. The life expectancy, or the time before someone successfully hacks, a default installation of Red Hat 6.2 server is less than 72 hours. A common home user setup, with Windows 98 and file sharing enabled, was hacked





FOREWORD

five times in four days. Systems are subjected to NetBIOS scans an average of 17 times a day. And the fastest time for a server being hacked: 15 minutes after plugging it into the network.

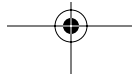
The moral of all of this is that there are a staggering number of people out there trying to break into *your* computer network, every day of the year, and that they succeed surprisingly often. It's a hostile jungle out there, and network administrators that don't take drastic measures to protect themselves are toast.

The Honeynet Project is more than a decoy network of computers; it is an ongoing research project into the modus operandi of predatory hackers. The project currently has several honeynets in operation. Want to try this in your own network? Several companies sell commercial, much simpler, versions of what the Honeynet Project is doing. Called "honeypots," they are designed to be installed on an organization's network as a decoy. In theory, hackers find the honeypot and waste their time with it, leaving the real network alone.

This acts as a network alarm. If you are monitoring your network alarms 24/7, or you have a Managed Security Monitoring service, then a honeypot can buy you valuable time to respond to attacks as they happen. The sophisticated attackers will probably avoid the honeypot, but most real-world attackers are amateurs. The key here is real-time monitoring; looking at the log files a week after the fact isn't much use.

For this reason, I am not sold on this as a commercial product. Honeynets and honeypots need to be tended; they're not the kind of product you can expect to work out of the box. Commercial honeypots only mimic an operating system or computer network; they're hard to install correctly and much easier to detect than the Honeynet Project's creations. And the security it buys you is incremental. If you're interested in learning about hackers and how they work, by all means purchase a honeypot and take the time to use it properly. But if you're just interested in protecting your own network, most of the time you'd be better off spending the time on other things.

The Honeynet Project, on the other hand, is pure research. And I am a major fan. The stuff they produce is invaluable, and there's no other practical way to get it.





FOREWORD

When an airplane falls out of the sky, everyone knows about it. There is a very public investigation, and any airline manufacturer can visit the National Traffic Safety Board and read the multi-hundred page reports on all recent airline crashes. And any airline can use that information to design better aircraft. When a network is hacked, it almost always remains a secret. More often than not, the victim has no idea he's been hacked. If he does know, there is enormous market pressure on him not to go public with the fact. And if he does go public, he almost never releases detailed information about how the hack happened and what the results were.

This paucity of real information makes it much harder to design good security products. This book is a major part of changing that. It talks about how their Honeynet works and how to analyze the data it produces, but is also synthesizes what they've learned so far: the tools, tactics, and motives of the "blackhat community" (i.e., malicious hackers).

This book is for anyone interested in computer security. Great stuff, and it's all real.

Bruce Schneier
<http://www.schneier.com>



