Chapter 5 Illegitimate Network Access

Chapter 5 Objective

This chapter will discuss:

- The "profiles" of those who illegitimately access systems,
- The various ways in which a user may illegitimately access an organization's network, and
- The various technical means an intruder may use to collect information or damage a target system.

5.1 Introduction

While there have been great strides in protecting ones networks, there remains a never-ending battle between those who wish to protect information those who wish to penetrate systems. Not all who penetrate systems do so maliciously, at least in their point of view, but from an organization's perspective anything that could cause damage is by its very nature malicious.

5.2 The Profiles

The human mind works best when it is able to segment people and things into clear groups. This is a fallacy, as no two people are alike and no two people are motivated identically. When considered in a broad context and used simply for discussion purposes, however, certain profiles of attackers hold true for someone in charge of defending an organization's IT systems.

5.2.1 Criminals

Criminal hackers are very dangerous because of their newfound ability to work together and to leverage high levels of education. Unfortunately,

as will be discussed in future chapters, criminals are not the "lone wolves" of the traditional hacking scene. Instead, they leverage their various skills in order to build more and better tools. It has long been suspected that various organized crime syndicates are involved in this, which makes the prospect even more frightening because they don't tend to give up.

5.2.2 Industrial Spies

Industrial espionage has been going on since industry began, but the new era of technology means those wishing to gain access to information have more and more opportunities. As will be discussed in Chapter 12, social engineering is a very effective technique used to trick an organization's employees to provide information on proprietary projects or even on people for use in short-cutting the research and development process or in enabling identity theft.

5.2.3 Ideologues

In a world of political moderates, the ability of people to affect change or at least gain publicity for their deeply-held beliefs strictly through their motivation to do so is astounding. Many protestors, such as those opposing western-style economic policies in developing countries, have been able to hack into sites to post their messages of protest, as well as being able to coordinate their protests over the Web, without meeting face-to-face.

5.2.4 Insiders

The threat of an insider abusing privilege is a major concern, as these people have been deemed as trustworthy by the organization in the past and have been granted access to the organization's networks. Unfortunately, when these employees become unhappy with their lot in life with the organization, an easy way for them to lash out is to abuse privilege or to commit a crime from within the walls of the organization itself.

5.2.5 Script Kiddies

Script kiddies are an annoyance but have the ability to cause real damage. This type of hacker is someone who is unable to or chooses not to develop their own exploits, but rather downloads them from the web and deploys them "out of the box."