to his time served. He is now an independent information security consultant and author.

Also in 1995, Russian hacker Vladimir Leven and associates performed electronic transfers of $10 million to a number of international banks. Leven was captured and tried in the U.S. and sentenced to three years' confinement. In 1998, "The Cult of the Dead Cow" announced and released very effective Trojan horse software called Back Orifice at Def Con. Back Orifice provided remote access to Windows 98 and Windows 95 computers.

In February 2000, hackers launched Distributed DoS attacks against Yahoo!, Amazon.com, and ZDNet. Microsoft Corporation's network was hacked in October 2000 by an attacker who gained access to software under development.

Ethical Hacking Objectives and Motivations

An ethical hacker attempts to duplicate the intent and actions of malicious hackers without causing harm. Ethical hackers conduct *penetration tests* to determine what an attacker can find out about an information system, whether a hacker can gain and maintain access to the system, and whether the hacker's tracks can be successfully covered without being detected.

The ethical hacker operates with the permission and knowledge of the organization they are trying to defend and tries to find weaknesses in the information system that can be exploited. In some cases, to test the effectiveness of their information system security team, an organization will not inform their team of the ethical hacker's activities. This situation is referred to as operating in a *double blind* environment.

To operate effectively, the ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support the ethical hacker's efforts.

Steps in Malicious Hacking

Hacking with malicious intent comprises the following steps, as shown in Figure 1-1:

1. Reconnaissance
   a. Active
   b. Passive

2. Scanning
3. Gaining access
   a. Operating system level
   b. Application level
   c. Network level
   d. Denial of service
4. Maintaining access
   a. Uploading programs/data
   b. Downloading programs/data
   c. Altering programs/data
5. Covering, clearing tracks, and installing back doors

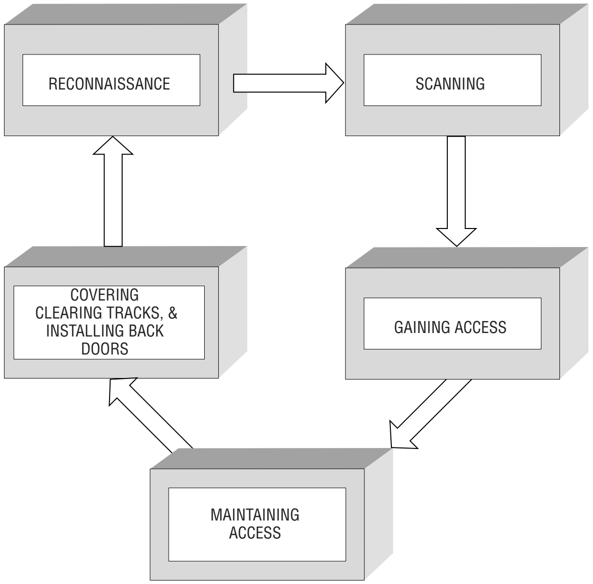

Figure 1-1: Malicious hacking steps