**Back Door or Trap Door** A virus or worm can have a payload that installs a back door or trap door component in a system, which allows the attacker to access the system at will with special privileges. Examples of these kinds of payloads include Subseven and Back Orifice.

**Polymorphic Threats** One of the biggest challenges to fighting viruses and worms has been the emergence of polymorphic threats. A polymorphic threat is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and other external file characteristics to elude detection by antivirus software programs.

**Virus and Worm Hoaxes** As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus hoaxes. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don’t exist. When people fail to follow virus-reporting procedures, the network becomes overloaded, and much time and energy is wasted as users forward the warning message to everyone they know, post the message on bulletin boards, and try to update their antivirus protection software

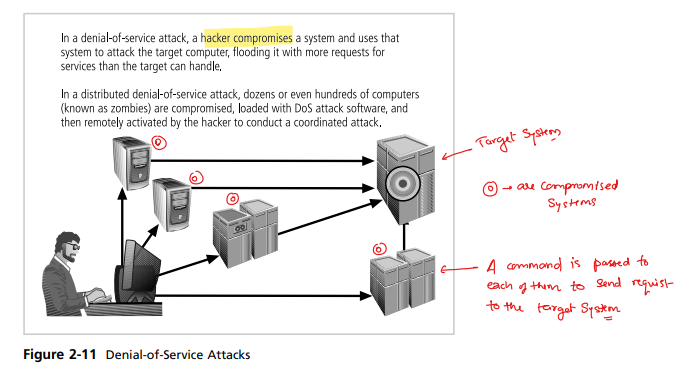
**Attack**

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)**

In a denial-of-service (DoS) attack, the attacker sends a large number of connection or information requests to a target (see Figure 2-11). So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service. The system may crash or simply become unable to perform ordinary functions.

A distributed denialof-service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into zombies, machines that are directed remotely (usually by a transmitted command) by the attacker to participate in the attack.

DDoS attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply. There are, however, some cooperative efforts to enable DDoS defenses among groups of service providers; among them is the Consensus Roadmap for Defeating Distributed Denial of Service Attacks.35 To use a popular metaphor, DDoS is considered a weapon of mass destruction on the Internet.36 The MyDoom worm attack of early 2004 was intended to be a DDoS attack against www.sco.com (the Web site of a vendor of a UNIX operating system) that lasted from February 1, 2004 until February 12, 2004. Allegedly, the attack was payback for the SCO Group’s perceived hostility toward the open-source Linux community.37 Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is vulnerable to DoS attacks. DoS attacks can also be launched against routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo).

****

**Brute Force** The application of computing and network resources to try every possible password combination is called a brute force attack. Since the brute force attack is often used to obtain passwords to commonly used accounts, it is sometimes called a password attack. If attackers can narrow the field of target accounts, they can devote more time and resources to these accounts. That is one reason to always change the manufacturer’s default administrator account names and passwords. Password attacks are rarely successful against systems that have adopted the manufacturer’s recommended security practices. Controls that limit the number of unsuccessful ac