

ATTACKS =

MOTIVE + METHOD +

VULNERABILITY

The method in this formula exploits the organization's vulnerability in order to launch an attack. Malicious attackers can gain access or deny services in numerous ways.

Here are some of them:

- **Viruses.** Attackers can develop harmful code known as viruses. Using hacking techniques, they can break into systems and plant viruses. Viruses in general are a threat to any environment. They come in different forms and although not always malicious, they always take up time. Viruses can also be spread via e-mail and disks.
- **Trojan horses.** These are malicious programs or software code hidden inside what looks like a normal program. When a user runs the normal program, the hidden code runs as well. It can then start deleting files and causing other damage to the computer. Trojan horses are normally spread by e-mail attachments. The Melissa virus that caused denial-of-service attacks throughout the world in 1999 was a type of Trojan horse.
- **Worms.** These are programs that run independently and travel from computer to computer across network connections. Worms may have portions of themselves running on many different computers. Worms do not change other programs, although they may carry other code that does.
- **Password cracking.** This is a technique attackers use to surreptitiously gain system access through another user's account. This is possible because users often select weak passwords. The two major problems with passwords is when they are easy to guess based on knowledge of the user (for example, wife's maiden name) and when they are susceptible to dictionary attacks (that is, using a dictionary as the source of guesses).
- **Denial-of-service attacks.** This attack exploits the need to have a service available. It is a growing trend on the Internet because Web sites in general are open doors ready for abuse. People can easily flood the Web server with communication in order to keep it busy. Therefore, companies connected to the Internet should prepare for (DoS) attacks. They also are difficult to trace and allow other types of attacks to be subdued.
- **E-mail hacking.** Electronic mail is one of the most popular features of the Internet. With access to Internet e-mail, someone can potentially correspond with any one of millions of people worldwide. Some of the threats associated with e-mail are:

- **Impersonation.** The sender address on Internet e-mail cannot be trusted because the sender can create a false return address. Someone could have modified the header in transit, or the sender could have connected directly to the Simple Mail Transfer Protocol (SMTP) port on the target computer to enter the e-mail.
- **Eavesdropping.** E-mail headers and contents are transmitted in the clear text if no encryption is used. As a result, the contents of a message can be read or altered in transit. The header can be modified to hide or change the sender, or to redirect the message.
- **Packet replay.** This refers to the recording and retransmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences, because an intruder could replay legitimate authentication sequence messages to gain access to a system. Packet replay is frequently undetectable, but can be prevented by using packet time stamping and packet sequence counting.
- **Packet modification.** This involves one system intercepting and modifying a packet destined for another system. Packet information may not only be modified, it could also be destroyed.
- **Eavesdropping.** This allows a cracker (hacker) to make a complete copy of network activity. As a result, a cracker can obtain sensitive information such as passwords, data, and procedures for performing functions. It is possible for a cracker to eavesdrop by wiretapping, using radio, or using auxiliary ports on terminals. It is also possible to eavesdrop using software that monitors packets sent over the network. In most cases, it is difficult to detect eavesdropping.
- **Social engineering.** This is a common form of cracking. It can be used by outsiders and by people within an organization. Social engineering is a hacker term for tricking people into revealing their password or some form of security information.
- **Intrusion attacks.** In these attacks, a hacker uses various hacking tools to gain access to systems. These can range from password-cracking tools to protocol hacking and manipulation tools. Intrusion detection tools often can help to detect changes and variants that take place within systems and networks.
- **Network spoofing.** In network spoofing, a system presents itself to the network as though it were a different system (computer A impersonates computer B by sending B's address instead of its own). The reason for doing this is that systems tend to operate within a group of other trusted systems. Trust is imparted in a one-to-one fashion; computer A trusts computer B (this does not imply that system B trusts system A). Implied with this trust is that the system administrator of the trusted system is performing the job properly and maintaining an appropriate level of security for the system. Network spoofing occurs in the following manner: if computer A trusts computer B and computer C spoofs (impersonates) computer B, then computer C can gain otherwise-denied access to computer A.