Malicious Attack

An **attack** on a computer system or network asset succeeds by exploiting a vulnerability in the system. There are four general categories of attack. An attack can consist of all or a combination of these four categories:

Fabrications—Fabrications involve the creation of some deception in order to trick unsuspecting users.

Interceptions—An interception involves eavesdropping on transmissions and redirecting them for unauthorized use.

Interruptions—An interruption causes a break in a communication channel, which blocks the transmission of data.

• **Modifications**—A modification is the alteration of data contained in transmissions or files.

As you learned earlier, security threats can be active or passive. Both types can have negative repercussions for an IT infrastructure. An active attack involves a modification of the data stream or attempts to gain unauthorized access to computer and networking systems. An active attack is a physical intrusion. In a passive attack, the attacker does not make changes to the system. This type of attack simply eavesdrops on and monitors transmissions.

Active threats include the following:

Birthday attacks
Brute-force password attacks
Dictionary password attacks
IP address spoofing
Hijacking
Replay attacks
Man-in-the-middle attacks
Masquerading
Social engineering
Phishing
Phreaking
Pharming

Such attacks are widespread and common. A growing number of them appear on information systems security professionals' radar screens every year. Following is a description of several of the most common types of malicious attacks.

Birthday Attacks

Once an attacker compromises a hashed password file, a **birthday attack** is performed. A birthday attack is a type of cryptographic attack that is used to make brute-force attack of one-way hashes easier. It is a mathematical exploit that is based on the birthday problem in probability theory.

Brute-Force Password Attacks

One of the most tried-and-true attack methods is the brute-force password attack. In a brute-force password attack, the attacker tries different passwords on a system until one of them is successful.

Usually the attacker employs a software program to try all possible combinations of a likely password, user ID, or security code until it locates a match. This occurs rapidly and in sequence. This type of attack is called a *brute-force password attack* because the attacker simply hammers away at the code. There is no skill or stealth involved—just brute force that eventually breaks the code.

With today's large-scale computers, it is possible to try millions of combinations of passwords in a short period. Given enough time and using enough computers, it is possible to crack most algorithms.

Dictionary Password Attacks

A *dictionary password attack* is a simple attack that relies on users making poor password choices. In a dictionary password attack, a simple password-cracker program takes all the words from a dictionary file and attempts to log on by entering each dictionary entry as a password.

Users often engage in the poor practice of selecting common words as passwords. A password policy that enforces complex passwords is the best defense against a dictionary password attack. Users should create passwords composed of a combination of letters and numbers, and the passwords should not include any personal information about the user.

IP Address Spoofing

Spoofing is a type of attack in which one person, program, or computer disguises itself as another person, program, or computer to gain access to some resource. A common spoofing attack involves presenting a false network address to pretend to be a different computer. An attacker may change a computer's network address to appear as an authorized computer in the target's network. If the administrator of the target's local router has not configured it to filter out external traffic with internal addresses, the attack may be successful. IP address spoofing can enable an attacker to access protected internal resources.

Address resolution protocol (ARP) poisoning is an example of a spoofing attack. In this attack, the attacker spoofs the MAC address of a targeted device, such as a server, by sending false ARP resolution responses with a different MAC address. This causes duplicate network traffic to be sent from the server. Another type of network-based attack is the **Christmas (Xmas) attack**. This type of attack sends advanced TCP packets with flags set to confuse IP routers and network border routers with TCP header bits set to 1, thus lighting up the IP router like a Christmas tree.

Hijacking

Hijacking is a type of attack in which the attacker takes control of a session between two machines and masquerades as one of them. There are a few types of hijacking:

Man-in-the-middle hijacking—In this type of hijacking, discussed in more detail in a moment, the attacker uses a program to take control of a connection by masquerading as each end of the connection. For example, if Mary and Fred want to communicate, the attacker pretends to be Mary when talking with Fred and pretends to be Fred when talking to Mary. Neither Mary nor Fred know they are talking to the attacker. The attacker can collect substantial information and can even alter data as they flow between Mary and Fred. This attack enables the attacker to either gain access to the messages or modify them before retransmitting. A man-in-the-middle attack can occur from an insider threat. An insider threat can occur from an employee, contractor, or trusted person within the organization.

Browser or URL hijacking—In a browser or **URL hijacking** attack, the user is directed to a different website than what he or she requested, usually to a fake page that the attacker has created. This gives the user the impression that the attacker has compromised the website when in fact the attacker simply diverted the user's browser from the actual site. This type of attack is also known as **typo squatting**. Attackers can use this attack with phishing to trick a user into providing private information such as a password. (You'll learn about phishing in a moment.)

- **Session hijacking**—In **session hijacking**, the attacker attempts to take over an existing connection between two network computers. The first step in this attack is for the attacker to take control of a network device on the LAN, such as a firewall or another computer, in order to monitor the connection. This enables the attacker to determine the sequence numbers used by the sender and receiver. After determining the sequence numbering, the attacker generates traffic that appears to come from one of the communicating parties. This steals the session from one of the legitimate users. To get rid of the legitimate user who initiated the hijacked session, the attacker overloads one of the communicating devices with excess packets so that it drops out of the session.

Replay Attacks

Replay attacks involve capturing data packets from a network and retransmitting them to produce an unauthorized effect. The receipt of duplicate, authenticated IP packets may disrupt service or have some other undesired consequence. Systems can be broken through replay attacks when attackers reuse old messages or parts of old messages to deceive system users. This helps intruders to gain information that allows unauthorized access into a system.

Man-in-the-Middle Attacks

A **man-in-the-middle attack** takes advantage of the multihop process used by many types of networks. In this type of attack, an attacker intercepts messages between two parties before transferring them on to their intended destination.

Web spoofing is a type of man-in-the-middle attack in which the user believes a secure session exists with a particular web server. In reality, the secure connection exists only with the attacker, not the web server. The attacker then establishes a secure connection with the web server, acting as an invisible go-between. The attacker passes traffic between the user and the web server. In this way, the attacker can trick the user into supplying passwords, credit card information, and other private data.

Attackers use man-in-the-middle attacks to steal information, to execute DoS attacks, to corrupt transmitted data, to gain access to an organization's internal computer and network resources, and to introduce new information into network sessions.

Masquerading

In a **masquerade attack**, one user or computer pretends to be another user or computer. Masquerade attacks usually include one of the other forms of active attacks, such as IP address spoofing or replaying. Attackers can capture authentication sequences and then replay them later to log on again to an application or operating system. For example, an attacker might monitor usernames and passwords sent to a weak web application. The attacker could then use the intercepted credentials to log on to the web application and impersonate the user.

Eavesdropping

Eavesdropping, or sniffing, occurs when a host sets its network interface on promiscuous mode and copies packets that pass by for later analysis. Promiscuous mode enables a network device to intercept and read each network packet, even if the packet's address doesn't match the network device. It is possible to attach hardware and software to monitor and analyze all packets on that segment of the transmission media without alerting any other users. Candidates for eavesdropping include satellite, wireless, mobile, and other transmission methods.

Social Engineering

Attackers often use a deception technique called **social engineering** to gain access to resources in an IT infrastructure. In nearly all cases, social engineering involves tricking authorized users into carrying out actions for unauthorized users. The success of social engineering attacks depends on the basic tendency of people to want to be helpful.

Social engineering places the human element in the security breach loop and uses it as a weapon. A forged or stolen vendor or employee ID could provide entry to a secure location. The intruder could then obtain access to important assets. By appealing to employees' natural instinct to help a technician or contractor, an attacker can easily breach the perimeter of an organization and gain access.

Personnel who serve as initial contacts within an organization, such as receptionists and administrative assistants, are often targets of social engineering attacks. Attackers with some knowledge of an organization's structure will often also target new, untrained employees as well as those who do not seem to understand security policies.

Eliminating social engineering attacks can be difficult, but here are some techniques to reduce their impact:

Ensure that employees are educated on the basics of a secure environment.

Develop a security policy and computer use policy.

Enforce a strict policy for internal and external technical support procedures.

Require the use of identification for all personnel.

Limit the data accessible to the public by restricting the information published in directories, Yellow Pages, websites, and public databases.

Be very careful when using remote access. Use strong validation so you know who is accessing your network.

Teach personnel the techniques for sending and receiving secure email.

Shred all documents that may contain confidential or sensitive information.

Phreaking

Phone phreaking, or simply **phreaking**, is a slang term that describes the activity of a subculture of people who study, experiment with, or explore telephone systems, telephone company equipment, and systems connected to public telephone networks. Phreaking is the art of exploiting bugs and glitches that exist in the telephone system.

Phishing

Fraud is a growing problem on the Internet. **Phishing** is a type of fraud in which an attacker attempts to trick the victim into providing private information such as credit card numbers,

passwords, dates of birth, bank account numbers, automated teller machine (ATM) PINs, and Social Security numbers.

A phishing scam is an attempt to commit identity theft via email or instant message. The message appears to come from a legitimate source, such as a trusted business or financial institution, and includes an urgent request for personal information. Phishing messages usually indicate a critical need to update an account (banking, credit card, etc.) immediately. The message instructs the victim to either provide the requested information or click on a link provided in the message. Clicking the link leads the victim to a spoofed website. This website looks identical to the official site but in fact belongs to the scammer. Personal information entered into this web page goes directly to the scammer, not to the legitimate organization.

A variation of the phishing attack is spear phishing. **Spear phishing** uses email or instant messages to target a specific organization, seeking unauthorized access to confidential data. As with the messages used in regular phishing attempts, spear-phishing messages appear to come from a trusted source.

The best way to protect against phishing of any kind is to avoid clicking on a link directly provided by a suspect email. Supplying personal information when prompted to do so by an email or instant message is too easily done once the website is in front of you. If you believe the request might be legitimate, call the company's customer service department to verify the request before providing any information. If you do call the company, do not use any phone numbers contained in the suspect message. Even if the URL displayed in the message is legitimate, manually enter the web address in your browser rather than clicking on a link in the message.

The Anti-Phishing Working Group (APWG) is a global, pan-industrial law enforcement association focused on eliminating fraud and identity theft resulting from email spoofing of all types. For more information, visit the APWG website at *www.antiphishing.org*. In addition, the Federal Trade Commission (FTC) website (*www.ftc.gov*) offers advice for consumers and an email address for reporting phishing activity, plus a form to report identity theft.

Pharming

Pharming is another type of attack that seeks to obtain personal or private financial information through domain spoofing. A pharming attack doesn't use messages to trick victims into visiting spoofed websites that appear legitimate, however. Instead, pharming "poisons" a domain name on the domain name server (DNS), a process known as **DNS poisoning**. The result is that when a user enters the poisoned server's web address into his or her address bar, that user navigates to the attacker's site. The user's browser still shows the correct website, which makes pharming difficult to detect—and therefore more serious. Where phishing attempts to scam people one at a time with an email or instant message, pharming enables scammers to target large groups of people at one time through domain spoofing.