**Security Attacks**

1. Virus
2. Worm
3. Trojan horse
4. Sniffing
5. Spoofing--3 types(a)IP or Packet Spoofing (b) DNS spoofing

(c) ARP spoofing

1. Phishing
2. Pharming(DNS spoofing)
3. Eavesdropping
4. Modification
5. Denial of Service(DOS)
6. SYN attack of DOS
7. Brute Force Attack
8. Man in Middle attack

## Classes of Malicious Software

Two of the most common types of malware are viruses and worms. These types of programs are **able to self-replicate and can spread copies of themselves**, which might even be modified copies. To be classified as a virus or worm, **malware must have the ability to propagate**. The difference is that a **worm operates more or less independently of other files, whereas a virus depends on a host program to spread itself**. These and other classes of malicious software are described below.

### Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an [executable file](http://www.webopedia.com/TERM/e/executable_file.html), which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

**Worms**

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of [social engineering](http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29) to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

**Trojans**

A Trojan is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system.

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

**Brute Force Attack**

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

The following measures can be used to defend against brute force attacks:

* Requiring users to create complex passwords
* Limiting the number of times a user can unsuccessfully attempt to log in
* Temporarily locking out users who exceed the specified maximum number of failed login attempts

# Man-in-the-middle attack

In cryptography and [computer security](https://en.wikipedia.org/wiki/Computer_security), a **man-in-the-middle attack** (**MITM**) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of man-in-the-middle attacks is active [eavesdropping](https://en.wikipedia.org/wiki/Eavesdropping), in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.

