**Kinds of security breaches (penetration)**

**Vulnerability** is a weakness in the security system, for example, in procedures, design, or implementation that might be exploited to cause loss or harm.

**A threat** to a computing system is a set of circumstances that has the potential to cause loss or harm

A human who exploits vulnerability perpetrates an **attack** on the system. An attack can also be launched by another system.

**Kinds of threats**

1) **Interception:** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network.

2) **Interruption**: an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file or malfunction of an operating system file manager so that it cannot find a particular disk file.

3) **Modification** means an unauthorized party not only accesses but tampers with an asset,. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically.

4) **Fabrication**: an unauthorized party might create a fabrication of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database.

**Vulnerabilities of Computing Systems**

1) **Hardware Vulnerabilities**: Hardware is more visible than software, largely because it is composed of physical objects. Its simple to attack by adding devices, changing them, removing them. This type of attack might be considered as involuntary or voluntary machine slaughter:

**Involuntary machine slaughter**: accidental acts not intended to do serious damage to the hardware such that:electrocuted with power surges drenched with water and People have spilled soft drinks.

**Voluntary machine slaughter**: more serious attack usually involves someone who actually wishes to harm the computer hardware such as Machines have been shot with guns and stabbed with knives.

2) **Software Vulnerabilities**: Software can be replaced, changed, or destroyed maliciously, or it can be modified, deleted, or misplaced accidentally.

**Software Deletion**: Software is surprisingly easy to delete.Access to software is usually carefully controlled through a process called **configuration management** so that software cannot be deleted, destroyed, or replaced accidentally.

**Software Modification**: S/W easy to modify. Changing a bit or two can convert a working program into a failing one .Depending on which bit was changed, the program may crash when it begins or it may execute for some time before it falters.The program called **logic bomb** when this program maliciously modified to fail when certain conditions are met or when a certain date or time is reached.