

Sniffing

- It is a process of monitoring and capturing all data packets passing through a given network using software or a hardware .
- Attackers use sniffers to capture data containing sensitive information such as password ,account details etc.



Spoofing

- It happens when an attacker or malicious program successfully acts on another persons behalf by impersonating data .
- Example of spoofing** is when an email is sent from a unauthorized or false sender address, that asks the recipient to provide sensitive data. This email could also contain a link to a malicious website that contains malware.

TCP/IP hacking

- When an unauthorized person or user hack or hijack a network connection of another user .
- **For example** .the attacker monitors the network transmission and analyse the sources and destination IP address of the two computer .Once the attackers discovers the IP address of one of the user ,they can knock one of the users off their connections using a denial of services attack and then resume communication by spoofing the ip-address of the disconnected user .It is combination of sniffing and spoofing

SQL injection

- ❑ It is a techniques where malicious users can inject SQL commands into an SQL statement ,via web pages .
- ❑ Injected SQL commands can alter SQL commands or statement and compromise the security of a web application

Logic Bomb

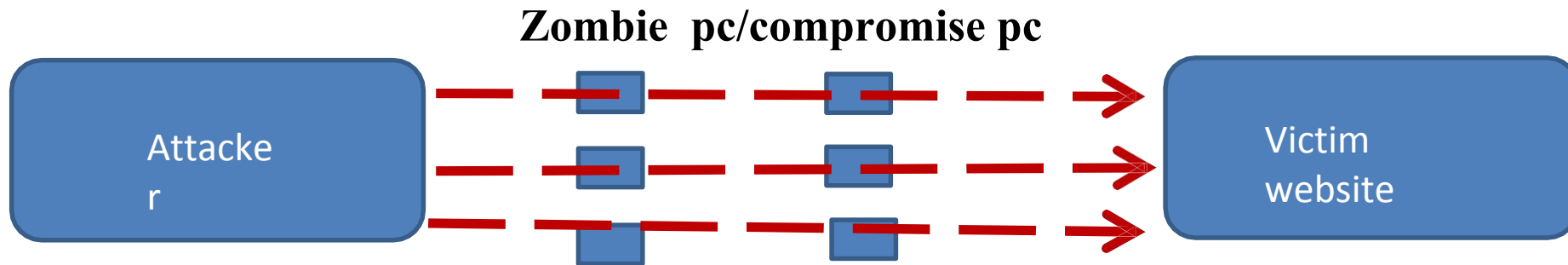
- It is some kind of triggered code or program which is embedded in any important software that is to explode when certain condition are met .
- The condition can be anything like any presence of file or absence of file ,or it can be just act like a time bomb which is set according to a particular time or a day .

Phishing attack

- In this kind of attack the hacker created a fake account or a fake website that looks exactly same as the original one .
- When the users attempt to log in his /her details, hackers records their data and used for its own purpose

Distributed denial of services (DDos)

- Ddos attack means using several computers and connections .the computers behind such as attack are often distributed around the world and will be a part of BOTNET.(zombie system)

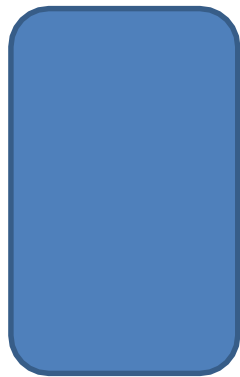


Man in the middle attack

- In this kind of attack the attacker secretly relays and possibly alters the communications b/w two parties who believe they are directly communicating with each other .

Trojan horse

- ❑ Its alike a virus.
- ❑ But doesn't modify the data and also doesn't replicate the data.
- ❑ It's a hidden kind of code which is intended to leak your confidential data /message or information.



login



Password



When you entered your password and id the trojan horse is reading the keys you are typing and after that it take a record/snapshot.