Phishing:

Phishing can be defined as an e-mail fraud method, where an individual group try to obtain financial or other confidential information from internet users, typically by sending an email that looks as if it is from a legitimate organisation like PayPal, eBay or Yahoo, but contain a link to a fake website that replicates the real one.

Fake Helpdesk calls to users:

The scam usually begins with an email or a cold call with the contact representing themselves as a help desk employee from a legitimate software or hardware vendor. The bogus representative tries to convince victims that their computers are malfunctioning, sometimes using a computer log that shows a lot of mostly harmless or low level errors. They then convince the victim to download software or let the "technician" remotely access their machines.

Password Attacks:

EASY PASSWORDS:

-The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always as difficult as you'd expect. Most networks aren't configured to require long and complex passwords, and an attacker needs to find only one weak password to gain access to a network. Not all authentication protocols are equally effective against guessing attacks. For example, because LAN Manager authentication is case-insensitive, a password guessing attack against it doesn't need to consider whether letters in the password are uppercase or lowercase.

Many tools can automate the process of typing password after password. Some common password guessing tools are Hydra, for guessing all sorts of passwords, including HTTP, Telnet, and Windows logons; TSGrinder Services and RDP connections; and SQLRecon , for brute-force attacks against SQL authentication.

Automated password guessing programs and crackers use several different approaches. The most time consuming—and most successful—attack method is the **brute-force attack**, in which the attacker tries every possible combination of characters for a password, given a character set (e.g., abcd...ABCD...1234...!@#$) and a maximum password length.

Dictionary attacks work on the assumption that most passwords consist of whole words, dates, or numbers taken from a dictionary. Dictionary attack tools require a dictionary input list. You can download varying databases with specific vocabularies (e.g., English dictionary, sports, even Star Wars trivia) free or commercially off the Internet.

Denial of services:

DOS is "Disk Operating System" or "Denial Of Service(attack)". Dos was the first widely installed operating system for personal computer.The first personal computer version of DOS, called PC-DOS, was developed for IBM by Bill Gates and his new microsoft corporation. He retained the rights to market a Microsoft version, called MS-DOS. PC-DOS and MS-DOS are almost identical and most users have referred to either of them as just "DOS".

SYN flood is an attack vector for conducting a denial-of-service (DOS) attack on a computer server. The attack involves having a client repeatedly send SYN (synchronization) packet to every port on a server, using fake IP address.

DDOS (distributed denial-of-services) is one in which a multitude of compromised system attack a single target,thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Unlike a computer virus, it doesn’t need to attach itself to an existing program. Worms almost always cause at least some harm to the host network , even if by only consuming bandwidth. It donot need human action to spread , it can replicate itself and get hundred or thousand of copies sended to any of the email we are in contact with creating a huge devastating effect. Computer worms can also contain “payloads” that damage host computers. Payloads are pieces of code written to perform actions affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data or delete files.

Viruses

A computer virus attaches itself to program or a file enabling it to spread from one computer to another , leaving infections as it travels. Some virus just cause annoying effects while other can cause serious problem in our hardware, software or files. Most of the viruses are attached to an executable file , which means it may exist on our computer but it cannot cause cause damage until we open or run it. A virus cannot spread without human action because it only spread when people unknowingly run a unknown program or share infected files or sending emails with virus attached files.

Trojan horse

A Trojan horse is full of as much trickery as trojan horse appeared in myths which it was named after. IT seems to be any useful software at first due to which we install or run it in our computer and it actually harms or damage our computer system. All the activated trojan horse in computer donot result the same. Some Trojan horse s just cause annoying effects like adding silly active desktop icons whereas some can cause serious damage by deleting files and destroying information on our system. It is not like viruses and worms , it don’t reproduce by infecting other files nor do they self replicate.