SECURITY THREATS AND ATTACKS

Definition of security threats and attacks.

Security threats

These refer to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage.

Security attacks

These involve an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations.

Security threats to information security are outlined as below;

1.Computer viruses - Pieces of software that are designed to spread from one computer to another that change the normal functionality of files and programs. They are often sent as email attachments or downloaded from specific websites with the intent to infect computers by using systems on a network. They send spam,disable security settings, corrupt and steal data such as passwords and can also delete data from a hard drive.

2. Rogue security software - This is malicious software that misleads users to believe that there is a computer virus installed on their computer or that security measures and installed antivirus software is not up to date. Users are offered installation or security settings update by downloading these programs to remove alleged viruses and as such this leads to actual malware being installed onto a computer.

3. Trojan horse - This is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate piece of software package. Often they spread through emails which come with attachments that are downloaded with malware onto a computer. Also spread through false online advertisements.

4. Adware and Spyware - Adware is software designed to track browsing habits which it uses to show advertisements and pop-ups. It collects data with consent. It is noticeable in pop ups and sometimes can slow down a computer's processor and internet connection speed. If downloaded without consent it's considered malicious while Spyware als works the same but is installed without a user's knowledge and it can contain keyloggers that record personal information such as email addresses and passwords which have a high risk of identity theft.

5. Computer worms - These are pieces of malware programs that replicate quickly and spread from one computer to another. They send themselves from infected computers to non-infected computers via networks and contacts.

6. DOS (Denial Of Service) and DDOS (Distributed Denial Of Service) attack - DOS is a malicious traffic overload that occurs when attackers overflood a website with traffic and as such it is unable to serve its content to visitors while a DDOS is more forceful and launched from several computers that are distributed from various locations.

7. Phishing - A method of social engineering with the goal of obtaining sensitive data such as passwords, usernames and credit card numbers. Often come in form of emails or messages that appear legitimate but containing malicious links.

8. Rootkit - This refers to a collection of software tools that enables remote control and administration level access over a computer or networks and once remote access is obtained, the rootkit can perform a number of malicious actions as they come with keyloggers, password stealers and antivirus disablers.

9. SQL Injection attack - These are attacks designed to target data driven applications by exploiting security vulnerabilities in the application's software. Malicious code is used to obtain private data, change and even destroying data.

10. Man in the middle - These are attacks that allow the attacker to eavesdrop on communication between two targets and can listen. The attacker intercepts communication between two parties.

11. Acts of human error failure - Accidents, employee mistakes
12. Compromise to intellectual property - Piracy, copyright infringement
13. Deliberate acts of espionage or trespass - Unauthorized access and data collection
14. Deliberate acts of information extortion - Blackmail of information disclosure
15. Deliberate acts of sabotage or vandalism - Destruction of systems & information
16. Deliberate acts of theft - Illegal confiscation of equipment or information
17. Forces of nature - Fires, Floods, earthquake, lightning

Security attacks to information security are outlined as below;
1.Malicious code - This is where execution of viruses, trojans and worms are used with the intent to modify, steal, or destroy information.

2. Backdoor - This is where unauthorized access is gained to a system or network using known or previously unknown access mechanisms.

3. Password Crack and brute force - This is an attempt to reverse calculate a password and gain access to at system or a network with also trying all possible combinations.

4. Dictionary - This attack selects specific accounts to attack and uses commonly used passwords with the dictionary as a guide for guessing.

5. Denial Of Service (DOS) - Attacker sends large number of connection or information requests to a system which make it not able to handle with other legitimate service requests and as such results into a crash or inability to function normally.

6. Distributed Denial Of Service (DDOS) - This is where a coordinated stream of requests is launched against a target system from many locations simultaneously resulting into crash or inability for normal functioning.

7. Spoofing - This is a technique used to gain unauthorized access where an intruder assumes a trusted IP address that is used to gain access to information.

8. Sniffers - These are programs or devices that monitor data traveling over networks and can be used both for legitimate purposes and for stealing information.

9. Social engineering - This refers to using social skills to convince people to reveal access credentials or other valuable information to attackers.

10. Masquerade – Masquerade attack takes place when one entity pretends to be different entity. For instance An attacker pretends to be the original sender of a message to the receiver.

11. Repudiation – This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has sent or received a message. For example, customer ask his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.

Conclusion.
Above are some of the different types of security threats and attacks.