SYN Flooding (DDOS) Attack:
SYN Flooding Attack occurs when adversary sends multiple SYN requests to server. In response server sends back SYN/ACK packets. Now, the ports on server side are listening. The main idea is for adversary to not send back ACK packets so server ports stay in listening mode – until timeout. Only after timeout, server ports are freed but adversary sends multiple requests so all server ports get busy and no port is available for communication with legitimate users.
There are three types of attacks that can be done this way. One is when adversary doesn't hide its IP and tries to do a DDOS attack. In this it is easier for server to detect the IP of attacker and block it. Second way is to use a botnet to send requests. Attacks are done with spoofed IP addresses. This makes it harder to detect attacker's identity but can be done eventually. Third way is DDOS in which different devices are used to send multiple SYN packets to server.

SCTP:
Stream Control Transmission Protocol is a transport layer protocol which has functionalities of TCP as well as UDP protocols. It's a message-oriented protocol like UDP which means it sends message in a way that receiver understands one complete message has been sent. It can handle multiple streams simultaneously. It also provides multihoming which means it can use IP's from different ISP's for connection. If one ISP fails, another one can be used to continue transmission. For transmissions it can detect connection beforehand. Like UDP it sends packet without any specific order. It has a 12-byte header. It does fragmentation of data to be sent like TCP. It uses Checksum mechanism for validation. It can also detect duplicate packets and corrupted packets. It can use maximum of eight source and eight destination IP addresses. For every session, policies are to be specified beforehand.
It is robust to man-in-the-middle and DDOS attacks by using cookie mechanism in the initial connection procedure. It doesn't allow half-open connections so SYN flooding attacks can be kept at bay. Cookie mechanism: Sender/attacker sends INIT packet, receiver sends INIT-ACK packet but with a cookie parameter with TCB information, along with signature for authentication. INIT-ACKs packets are always sent to sender so attacker doesn't receive it but legitimate users do. They then return the cookie in COOKIE ECHO chunk which servers can validate using their secret key which is known only to them.

TCP Timers:
There are four types of Timers: Time Out, Time Wait, Keep Alive, Persistent.
Time Out Timer is used for re-transmission of lost segments. Sender sends packet and starts the Time Out timer. If ACK is received before timeout period, the timer is stopped. If not then the packet is resent.
Time Wait Timer is used during connection termination. After sender sends second FIN's ACK, timer is started. If the ACK gets lost, it is sent again and timer is reset.
Keep Alive Timer is used to prevent long idle TCP connections. After server receives a packet from client, it sets the timer to two hours. If for two hours it doesn't receive any request from client, it sends ten segments to client to check whether client is up or not. If it doesn't receive a response, it knows the client is down so the connection is terminated.
Persistent Timer is used to keep track of zero-window-size situation. Let's say sender received a packet acknowledging the fact that receiver has no space in window to receive data. Now sender waits for window to have some space. Receiver got free space and sent and ACK but it got lost. Now sender and receiver both are in waiting state. To prevent this situation, Persistent timer is set.
