Denial of Service Attacks

DoS (Denial of service) attacks and DDoS (Distributed Denial of service) attacks are types of active attacks where the attacker seeks to render the targeted system to be unavailable to legitimate users. The underlying principle of the attack is that the attacker floods the victim's system with far more requests than it can handle, hence causing it to hang or even crash and won't be able to respond to legitimate requests. It is difficult to mitigate DoS as there is no way of differentiating between malicious and legitimate requests.

Types:

- Volumetric
  Here, the attacker floods the victim's network with huge volumes of request which are more than what the server can handle, hence consuming an excess amount of bandwidth.
  Example: UDP floods.

- Protocol
  A protocol attack is where the attacker exploits the server through the weakness of a particular protocol.
  Example: TCP SYN flood.

- Application
  These attacks target the Web-Application layer to attack the system.
  Example: Slowloris

- Amplification
  This is a special type of attack where the attacker asks for huge volumes of data by sending small requests but with the source IP spoofed as the victim's IP. Thus, huge amounts of data are sent to the victim and this causes the server to hang or crash.
  Example: DNS amplification attacks.

Mitigation

There is no way to completely mitigate DoS attacks as there is no way to differentiate between legitimate and malicious requests. The most common techniques would be to drop unresponsive connections, give timeouts for extremely slow connections and monitor huge sudden spikes of requests.