- **Packet sniffing: The practice of capturing and inspecting data packets across a network**
  - Active packet sniffing: A type of attack where data packets are manipulated in transit
  - Passive packet sniffing: A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network
- **Denial of service (DoS) attack: An attack that targets a network or server and floods it with network traffic. Has 3 types:**
  - Synchronize (SYN) flood attack: simulates a TCP/IP connection and floods a server with SYN packets
  - Internet Control Message Protocol (ICMP) flood: performed by an attacker repeatedly sending ICMP request packets to a network server
  - Ping of death: caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB
- Distributed denial of service (DDoS) attack: A type of denial of service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic
- **IP spoofing: A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network. Has 3 types:**
  - On-path attack: where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit
  - Replay attack: when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time
  - Smurf attack: when an attacker sniffs an authorized user's IP address and floods it with ICMP packets