Module 10 : CCNA - Security threat Landscape

1) Any type of malicious activity or attack that could potentially cause harm or damage to an organization, its data or its personnel.
2) Mitigation techniques aim to lower the potential impact of a risk and decrease the likelihood of the risk event from occurring.
3) A DoS (denial-of-service) attack is a cyberattack that makes a computer or other device unavailable to its intended users.
4) Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks.
5) IP spoofing is the creation of Internet Protocol (IP) packets which have a

modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both.

6) Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.

7) A man-in-the-middle attack is a cyberattack in which the attacker can secretly intercept messages between two or more parties who believe they are communicating with each other.