Module 10 CCNA - Security threat landscape

* **Beginner Question**

1. **Explain Security Threat**

* A security threat is a malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization. A security event refers to an occurrence during which company data or its network may have been exposed.

1. **What is mitigation Techniques?**

* Mitigation techniques are technologies used in radio communications to reduce the likelihood of interference from a radio transmitter to other users.
* **Intermediate Question**

1. **Explain DoS Attacks**

* A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users

1. **Explain DDoS**

* Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

1. **Explain IP spoofing**

* IP spoofing, or IP address spoofing, refers to the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system. IP spoofing allows cybercriminals to carry out malicious actions, often without detection.
* **Advance Question**

1. **What is social Engineering Attack?**

* Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

1. **Explain Man-In-The Middle Attack**

* A man-in-the-middle (MiTM) attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.