Module 10 CCNA - Security threat landscape

* ***Beginner Question***

1. ***Explain Security Threat***

***Ans.*** *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?***

***Ans.*** *Examples of mitigation strategies include: hazard specific control activities such as flood levees or bushfire mitigation strategies. design improvements to infrastructure or services. land use planning and design decisions that avoid developments and community infrastructure in areas prone to hazards.*

* ***Intermediate Question***

1. ***Explain DoS Attacks***

***Ans.*** *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 (i.e. employees, members, or account holders) of the service or resource they expected.*

1. ***Explain DDoS***

***Ans.*** *DDoS (Distributed Denial of Service) is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.*

1. ***Explain IP spoofing***

***Ans.*** *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?***

***Ans.*** *Social engineering is the term used for a broad range of* [*malicious activities accomplished through human interactions*](https://www.imperva.com/learn/application-security/malware-detection-and-removal/)*. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.*

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

***Ans.*** *A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.*