**Module 10 \\ LOKESH PANCHAL //**

**CCNA - Security threat landscape**

**• Beginner Question**

**1.** Explain Security Threat **Ans.** A security threat is a potential danger that can exploit vulnerabilities in a system, network, or organization, compromising its integrity, confidentiality, or availability. It encompasses various forms, such as malware, hacking, social engineering, and other malicious activities aimed at causing harm or unauthorized access.

**2.** What is mitigation Techniques? **Ans.** Mitigation techniques involve implementing proactive measures to minimize or prevent the impact of security threats. This includes measures like implementing strong access controls, regularly updating and patching software, conducting security audits, employing encryption, and educating users to enhance overall security posture.

• Intermediate Question

**1.**Explain DoS Attacks **Ans.** A Denial-of-Service (DoS) attack is a malicious attempt to disrupt a computer system, network, or service by overwhelming it with excessive traffic, rendering it temporarily or permanently unavailable to legitimate users.

**2.** Explain DDoS Ans. DDoS (Distributed Denial-of-Service) is an advanced form of DoS attack where multiple compromised devices are coordinated to flood a target system with overwhelming traffic, causing a severe service disruption.

3. Explain IP spoofing Ans. IP spoofing involves forging the source address in a network packet to deceive the recipient, often used in DDoS attacks to disguise the origin of malicious traffic and make it challenging to trace back to the attacker.

• Advance Question

**1.** What is social Engineering Attack? **Ans.** Social engineering is a deceptive tactic wherein attackers manipulate individuals to divulge confidential information or perform actions that compromise security, exploiting psychological vulnerabilities to gain unauthorized access or information. This often involves impersonation, trust exploitation, or emotional manipulation.

**2.** Explain Man-In-The Middle Attack **Ans.** A Man-in-the-Middle (MitM) attack involves an unauthorized third party intercepting and potentially altering communication between two entities, compromising the confidentiality and integrity of the data exchange. Attackers can eavesdrop, manipulate, or impersonate, posing a significant threat to secure communication.