Module 10 CCNA - Security threat landscape chirag panchal

• Beginner Question

1. Explain Security Threat

Ans- A security threat is a potential danger that can exploit vulnerabilities in a system or network, compromising its integrity, confidentiality, or availability

1. What is mitigation Techniques

Ans- Mitigation techniques involve implementing measures to reduce the impact and likelihood of security threats, enhancing the overall resilience of systems and networks

• Intermediate Question

1. Explain DoS Attacks

Ans- A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer system or network by overwhelming it with a flood of illegitimate traffic

1. Explain DDoS

Ans-Distributed Denial of Service (DDoS) is a cybar attack in which multiple compromised computers are used to flood a target system or network with excessive traffic, causing a disruption in service

1. Explain IP spoofing

Ans-IP spoofing is a technique where an attacker manipulates the source address in an IP packet to deceive a recipient, disguising the origin of the communication and potentially facilitating unauthorized access

• Advance Question

1.What is social Engineering Attack?

Ans-Social engineering is a manipulation technique used by attackers to exploit human psychology and deceive individuals into divulging confidential information or performing actions that compromise security

2. Explain Man-In-The Middle Attack

Ans-A Man-in-the-Middle (MitM) attack involves an unauthorized entity intercepting and potentially manipulating communication between two parties without their knowledge