2100031921
Kowshik
sec-54

Passive Attacks:
Passive attacks are security threats that involve unauthorized access to or observation of data without altering it. In these attacks, the attacker aims to gather information, often in secret, without directly affecting the target system's functionality. Passive attacks are difficult to detect because they don't cause noticeable disruptions. Examples of passive attacks include:

Eavesdropping: The attacker intercepts and listens to communication between parties, attempting to gather sensitive information such as passwords or confidential data.

Traffic Analysis: Attackers analyze patterns of communication traffic, even

without understanding the content, to deduce valuable information like user behaviors, relationships, or transaction timings.

monitoring: Unauthorized individuals monitor network traffic to gain insights into the activities of users, applications, or devices without altering the data being transmitted.

Passive Wiretapping: Attackers tap into communication lines to eavesdrop on data as it flows between devices, often using devices that don't alter the data stream.

Active Attacks:
Active attacks involve unauthorized manipulation or alteration of data, resulting in direct impact on the integrity, availability, or confidentiality of the targeted system or data. Active attacks disrupt the normal functioning of systems and can have more immediate and

noticeable effects. Examples of active attacks include:

Denial of Service (DoS) Attack: Attackers flood a system, network, or service with excessive traffic or requests, overwhelming its resources and causing it to become unavailable to legitimate users.

Distributed Denial of Service (DDoS) Attack: Similar to a DoS attack, but the attack traffic comes from multiple sources, making it even more challenging to mitigate.

malware Injection: Attackers insert malicious software (malware) into a system or network to compromise its security, steal data, or disrupt operations. This includes viruses, worms, Trojans, and ransomware.

man-in-the-middle (mitm) Attack: The attacker intercepts and possibly alters

communication between two parties without their knowledge, allowing them to steal sensitive information or manipulate data.

Phishing: Attackers use deceptive emails or websites to trick users into revealing sensitive information like passwords, credit card details, or personal information.

Data modification: Attackers alter data in transit or storage to manipulate its content, leading to unauthorized changes in information or incorrect decisions based on altered data.

Session Hijacking: Attackers take over an established user session to gain unauthorized access to systems, applications, or services.

Ransomware: malicious software encrypts a victim's data, and the attacker demands payment (ransom) for providing