










# Difference Between Active Attack and Passive Attack

Aspect	Active Attack	Passive Attack
 <b>Definition</b>	A deliberate attempt to alter, disrupt, or damage communication or system resources.	Unauthorized monitoring or interception of data without modifying it.
 <b>Primary Objective</b>	Breach data integrity, disrupt operations, manipulate or disable services.	Extract confidential information without alerting the victim.
 <b>Security Principles Impacted</b>	Integrity and Availability (part of CIA triad).	Confidentiality (part of CIA triad).
 <b>Visibility</b>	Often generates detectable anomalies, unusual traffic, session resets, service disruptions.	Typically stealthy and silent; difficult to detect without active monitoring.
 <b>Duration of Attack</b>	The duration of an active attack is short.	The duration of a passive attack is long.
 <b>Techniques Involved</b>	<ul style="list-style-type: none"><li>- Data tampering</li><li>- Session hijacking</li><li>- Replay attacks</li><li>- Man-in-the-Middle (MITM)</li><li>- Denial of Service (DoS) attacks</li></ul>	<ul style="list-style-type: none"><li>- Traffic sniffing</li><li>- Passive reconnaissance</li><li>- Packet capturing</li><li>- Wireless eavesdropping</li></ul>
 <b>Attacker Behavior</b>	Actively engages with the system or data stream to alter or disrupt.	Observes passively without interacting or leaving traces.
 <b>Detection and Response</b>	Easier to detect with Intrusion Detection Systems (IDS) and SIEM correlation rules.	Requires deep packet inspection, anomaly detection, and encrypted channels to uncover.
 <b>Real-world Scenarios</b>	<ul style="list-style-type: none"><li>- Altering DNS responses to redirect users</li><li>- Hijacking authenticated sessions</li><li>- Disrupting cloud services via targeted DoS attacks</li></ul>	<ul style="list-style-type: none"><li>- Monitoring corporate emails via compromised Wi-Fi</li><li>- Collecting intelligence during early-stage cyber espionage.</li></ul>