MITM

1. Man-in-the-middle (MITM) attacks: MITM attacks occur when an attacker intercepts communication between two parties, allowing them to eavesdrop or modify the communication without either party knowing.
   1. IP Spoofing: This attack involves an attacker sending a packet to a network with a false source IP address, making it appear as if the packet originated from a trusted source. This can be used to intercept traffic or launch other types of attacks.
   2. ARP Spoofing: This attack involves an attacker sending falsified Address Resolution Protocol (ARP) messages to a network, causing traffic to be redirected to the attacker's device instead of its intended destination.
   3. DNS Spoofing: This attack involves an attacker intercepting Domain Name System (DNS) requests and redirecting them to a fake website or server, allowing the attacker to steal sensitive information or launch other attacks.
   4. HTTPS Spoofing: This attack involves an attacker intercepting HTTPS traffic and using a fake SSL certificate to make the victim's browser believe that the website or server is legitimate, allowing the attacker to steal sensitive information.
   5. Wi-Fi Eavesdropping: This attack involves an attacker intercepting Wi-Fi traffic by setting up a rogue access point or by eavesdropping on a public Wi-Fi network, allowing the attacker to intercept and steal sensitive information.
2. MITM affecting casual internet users:
   1. Man-in-the-middle (MITM) attacks: These attacks are also able to affect all types of users. They can steal important information or intercept connections.