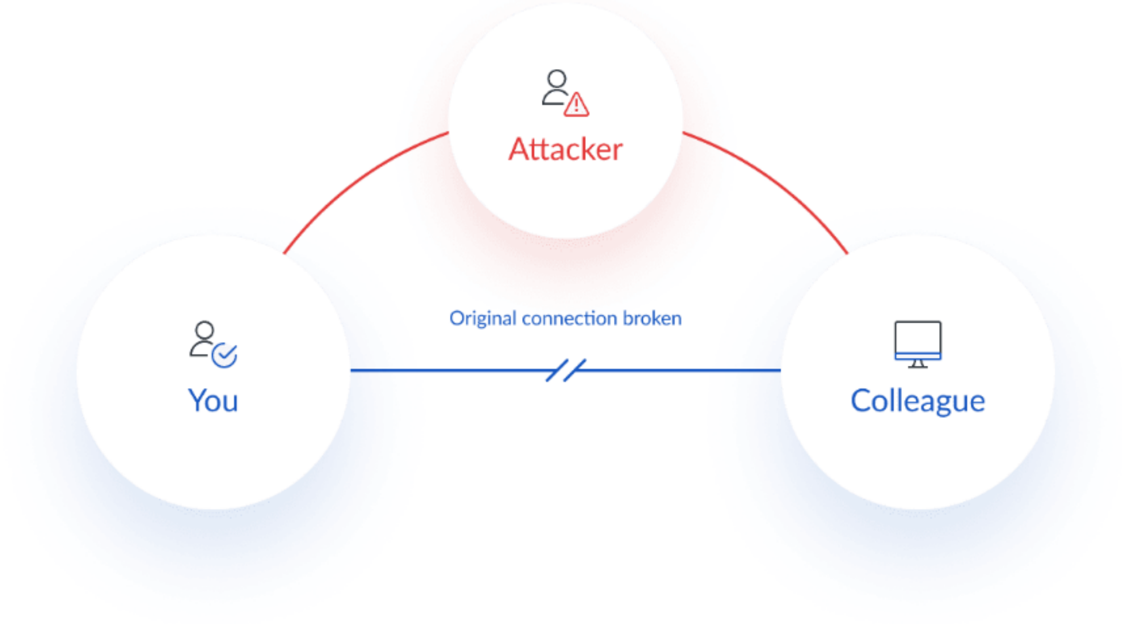
USE CASE



So the way the mitm work is by using ARP poisoning , so lets see what is ARP poisoning .

The Address Resolution Protocol (ARP) exists to support the layered approach used since the earliest days of computer networking. The functions of each layer, from the electrical signals that travel across an Ethernet cable to the HTML code used to render a webpage, operate largely independent of one another. This is how we can use IPv4 – a network layer technology dating to the early

1980s – with newer technologies like Wi-Fi and Bluetooth: The lower physical and data link layers handle the specifics of transferring data over a specific medium like radio waves.

The purpose of ARP is to translate between addresses at the data link layer – known as MAC Addresses – and addresses at the network layer, which are typically IP addresses. It allows networked devices to “ask” what device is currently assigned a given IP address.

Any device on the network can answer an ARP request, whether the original message was intended for it or not. For example, if Computer A “asks” for the MAC address of Computer B, an attacker at Computer C can respond and Computer A would accept this response as authentic. This oversight has made a variety of attacks possible. By leveraging easily available tools, a threat actor can “poison” the ARP cache of other hosts on a local network, filling the ARP cache with inaccurate entries.

So this way an attacker can act as the receiver and can sniff the data and then it can route it to the real target by modifying or monitor the traffic.

When the ARP poisoning is completed successfully now whatever the host want to send to the target will be completely visible by the hacker who is the man in the middle.