











Write up: ARP is a low level protocol which matches up with MAC addresses to IP addresses. If the IP address for a device is known but the MAC address is not, the sending computer sends an ARP packet to determine the MAC address. ARP poisoning relies upon MAC spoofing, which is impersonating another computer by means of changing the MAC address associated with an IP address. ARP poisoning is a kind of man in the middle security attack, and requires the attack is on the same network segment. Then the attacker can intercept all the traffic between those machines and the attackers computer can forwards the packets to their final destinations as it intercepts them. ARP tables are databases that reside on routers and keep records of which devices on the network correspond to which IP address. ARP poisoning is a king of man in the middle security attack, and requires the attack is on the same network segment. The way I simplify this is.. Imagine I'm trying to look at the mail two people are sending each other. If I manage to lie to the post office and have their mail forwarded to a couple of PO boxes in the post office, one for each, then I can read their mail. I can then put it in a new envelope and mail it to the recipients, and they'll never notice.