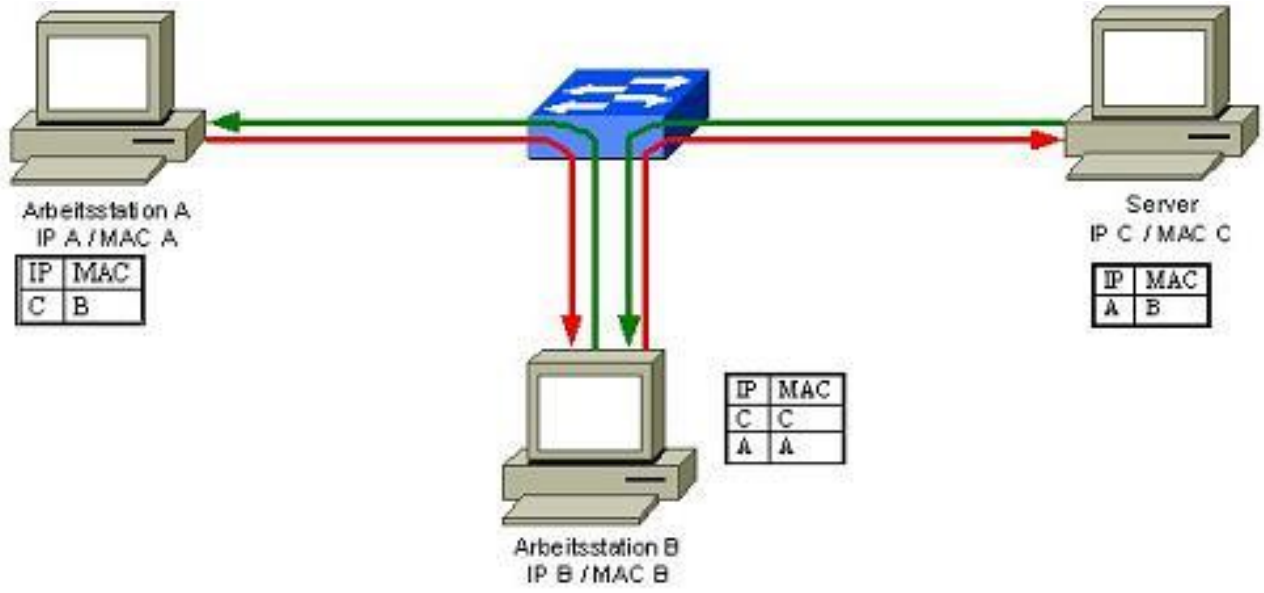
Angriffsmethoden: ARP – Spoofing

1. **Funktionsweise**

Das Address Resolution Protocol (ARP) dient in lokalen, auf Ethernet beruhenden Netzen der Zuordnung einer MAC-Adresse zu einer IP-Adresse. Die Kenntnis der IP-Adresse eines Servers allein genügt nicht, um mit ihm eine Verbindung aufzunehmen, denn alle TCP/IP-Pakete müssen ja in Ethernet-Frames transportiert werden. Deshalb muss ein Client zunächst die Ziel-MAC Adresse erfragen, indem er einfach per Broadcast die Frage stellt*: "Welche MAC-Adresse hat der Rechner mit der IP-Adresse B?" (ARP-Who-has)*. Der Rechner, mit dieser IP-Adresse antwortet darauf mit *"IP B ist unter MAC B zu erreichen"* an den Fragesteller. Um nicht jedes Mal nachfragen zu müssen, legt der Client die Zuordnung IP-MAC in einem lokalen ARP-Cache ab.

ARP bietet keine Funktionen, um sicherzustellen, dass die Antwort auch wirklich von dem Rechner kommt, mit dem man eine Verbindung aufbauen will. So kann prinzipiell jedes System im LAN vortäuschen, der Besitzer einer IP-Adresse zu sein. Zudem erlaubt das ARP-Protokoll die Verarbeitung von Antwort-Paketen, für die gar keine Anfrage gestellt wurde.

Ein Angreifer kann nun die Verbindung zwischen einem Client und Server oder Router über sich umleiten, indem er den Opfern manipulierte ARP-Replys mit seiner eigenen MAC-Adresse sendet. Dieses Einschleusen von gefälschten Adresspaaren in den Zwischenspeicher nennt man auch Cache-Poisoning. Anschließend schickt der angegriffene Client seine Pakete ohne weitere ARP-Anfragen immer zuerst an den Angreifer, der diese nach der Inspektion an den Server weiterleitet. Umgekehrt sendet der Server seine Antwort erst an den Angreifer, bevor dieser sie an den Client schickt. In solch einer **Man-in-the-Middle**-Position lässt sich fortan die gesamte IP-basierte Kommunikation zwischen den beiden Systemen mitlesen. Mit umgeleiteten Verbindungen kann ein Angreifer nicht nur etwa E-Mails und Zugangskennwörter ausspähen, sondern er kann auch Daten manipulieren. Besonders lohnende Ziele dafür sind Name-Server-Anfragen, da sich über sie auch die Kommunikation mit externen Servern umleiten lässt. Durch eine gefälschte DNS-Auskunft landet ein Opfer beispielsweise nicht auf dem eBay-Server, sondern auf einem präparierten System.



b) Schutz vor ARP – Spoofing

Eine einfache Möglichkeit PCs gegen ARP-Spoofing resistent zu machen, ist die Verwendung statischer ARP-Einträge (arp –s). Dies bedeutet aber, dass alle IP-Adressen mit den dazugehörigen MAC-Adressen von Kommunikationspartnern innerhalb einer Broadcast-Domain in den ARP-Cache eingetragen werden müssen. Das ist mit hohem administrativem Aufwand verbunden und in lokalen Netzen mit DHCP kaum möglich. Als Kompromiss kann der Netzadmin zumindest die MAC-Adresse des Standard-Gateways fest eintragen.

Arpwatch, ein Open-Source-Tool für UNIX-Plattformen, kann ARP-Pakete in einem lokalen Netz lesen, daraus die MAC-IP-Informationen entnehmen und speichern, sowie mit vorhanden Einträgen vergleichen. Nach einer Lernphase schlägt Arpwatch bei Paketen Alarm, die zu keinem Eintrag passen. Der Einsatz von Arpwatch eignet sich in kleineren Netzen, da sich der Aufwand dort noch in Grenzen hält.

Statischen ARP-Eintrag für das Standard-Gateway.