**3E. ARP Poisoning in Windows**

**What is ARP Poisoning:**

ARP Poisoning consists of abusing the weaknesses in ARP to corrupt the MAC-to-IP mappings of other devices on the network. Security was not a paramount concern when ARP was introduced in 1982, so the designers of the protocol never included authentication mechanisms to validate ARP messages. 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.

**Steps in ARP Poisoning:**

1. The first step in planning and conducting an ARP Poisoning attack is selecting a Target. This can be a specific endpoint on the network, a group of endpoints, or a network device like a router. Routers are attractive targets because a successful ARP Poisoning Attack against a router can disrupt traffic for an entire subnet.
2. A wide variety of tools are easily available to anyone looking to carry out an ARP Poisoning attack. After launching the tool of his or her choice and configuring applicable settings, the attacker will begin the attack. They may immediately begin broadcasting ARP messages, or wait until a request is received.
3. Once the ARP cache on a victim machine or machines has been corrupted, the attacker will typically perform some type of action with the incorrectly steered traffic. They may inspect it, alter it, or cause it to be “blackholed” and never reach its intended destination. The exact action depends on the attacker’s motives.

**Types of ARP Poisoning Attacks:**

1. Man-in-the-Middle (MiTM) Attack.
2. Denial of Service (DoS) Attack.
3. Session Hijacking.

**Aim of ARP Poisoning:**

Hackers have a wide [variety of motives](https://www.varonis.com/blog/hacker-motives/?hsLang=en), and ARP Poisoning is no exception. An attacker might carry out an ARP poisoning attack for any number of reasons, ranging from high-level espionage to the thrill of creating chaos on the network. In one potential scenario, an attacker will use falsified ARP messages to assume the role of the default gateway for a given subnet, effectively steering all traffic to the attacker’s machine instead of the local router. They may then spy on, modify, or drop the traffic. These attacks are “noisy” in the sense that they leave evidence behind, but they need not interfere with the actual operation of the network. If espionage is the goal, the attacking machine will simply forward the traffic to its original destination, giving the end-user no indication that anything has changed.

On the other hand, the point of a DoS attack might be to create a highly noticeable disruption in network operation. While this could be targeted at depriving a business of its ability to operate, DoS attacks are often carried out by less skilled attackers for the sheer enjoyment of creating problems.

**How to Prevent ARP Poisoning Attacks**

1. **Static ARP Tables**: It’s possible to statically map all the MAC addresses in a network to their rightful IP addresses. This is highly effective in preventing ARP Poisoning attacks but adds a tremendous administrative burden. Any change to the network will require manual updates of the ARP tables across all hosts, making static ARP tables unfeasible for most larger organizations. Still, in situations where security is crucial, carving out a separate network segment where static ARP tables are used can help to protect critical information.
2. **Switch Security**: Most managed Ethernet switches sport features designed to mitigate ARP Poisoning attacks. Typically known as Dynamic ARP Inspection (DAI), these features evaluate the validity of each ARP message and drop packets that appear suspicious or malicious. DAI can also typically be configured to limit the rate at which ARP messages can pass through the switch, effectively preventing DoS attacks.
3. **Physical Security**: Properly controlling physical access to your place of business can help mitigate ARP Poisoning attacks. ARP messages are not routed beyond the boundaries of the local network, so would-be attackers must be in physical proximity to the victim network or already have control of a machine on the network. Note that in the case of wireless networks, proximity doesn’t necessarily mean the attacker needs direct physical access; a signal extends to a street or parking lot may be sufficient. Whether wired or wireless, the use of technology like 802.1x can ensure that only trusted and/or managed devices can connect to the network.
4. **Network Isolation**: As stated previously, ARP messages don’t travel beyond the local subnet. This means that a well-segmented network may be less susceptible to ARP cache poisoning overall, as an attack in one subnet cannot impact devices in another. Concentrating important resources in a dedicated network segment where enhanced security is present can greatly diminish the potential impact of an ARP Poisoning attack.
5. **Encryption**: While encryption won’t actually prevent an ARP attack from occurring, it can mitigate the potential damage. A popular use of MiTM attacks was to capture login credentials that were once commonly transmitted in plain text. With the widespread use of SSL/TLS encryption on the web, this type of attack has become more difficult. The threat actor can still intercept the traffic, but can’t do anything with it in its encrypted form.