

ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks



Robert Grimmick

8 min read

Last updated August 4, 2022



ARP Poisoning is a type of cyberattack that abuses weaknesses in the widely used Address Resolution Protocol (ARP) to disrupt, redirect, or spy on network traffic. In this piece, we'll take a quick look at the need for ARP, the weaknesses that enable ARP Poisoning, and what you can do to keep your organization safe.

What is ARP?

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. Devices can also announce this mapping to the rest of the network without being prompted. For efficiency’s sake, devices will typically cache these responses and build a list of current MAC-to-IP mappings.

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.

ARP Poisoning Attack Steps

The exact steps of an ARP Poisoning attack can vary, but generally consist of at least the following:

Get the Free Pentesting Active Directory Environments e-book

First Name*
Last Name*

Email*

- I agree to receive communications from Varonis.
*

You can unsubscribe from these communications at any time. For more information on our privacy practices, and how we're committed to protecting your information, please review our [privacy policy](#).

1. Attacker Selects a Victim Machine or Machines

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. Attacker Launches Tools and Begins the Attack>

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. Attacker Does Something with the Incorrectly Steered Traffic

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

There are two general ways in which an ARP Poisoning attack can occur: The attacker can either wait to see ARP requests for a particular target and issue a response, or send out an unsolicited broadcast message known as a “gratuitous ARP”. The first approach is less noticeable on the network, but potentially less far-reaching in its impacts. A gratuitous ARP can be more immediate and impact a greater number of victims but comes with the downside of generating lots of network traffic. In either approach, the corrupted ARP cache(s) on victim machines may be leveraged to further ends:

Man-in-the-Middle (MiTM) Attack

[MiTM attacks](#) are probably the most common, and potentially most dangerous, goal of ARP poisoning. The attacker sends out falsified ARP responses for a given IP Address, typically the default gateway for a particular subnet. This causes victim machines to populate their ARP cache with the MAC address of the attacker’s machine, instead of the local router’s MAC address. Victim machines will then incorrectly forward network traffic to the attacker. Tools like Ettercap allow the attacker to act as a proxy, viewing or modifying information before sending the traffic to its intended destination. To the victim, everything may appear normal.

Marrying ARP Poisoning with [DNS Poisoning](#) can dramatically increase the effectiveness of a MiTM attack. In this scenario, a victim user might type in a legitimate site such as google.com and be given the IP address of the attacker’s machine, rather than the rightful address.

Denial of Service (DoS) Attack

A DoS attack is aimed at denying one or more victims access to network resources. In the case of ARP, an attacker might send out ARP Response messages that falsely map hundreds or even thousands of IP addresses to a single MAC address, potentially overwhelming the target machine. This type of attack, sometimes known as ARP flooding, can also be used to target switches, potentially impacting the performance of the entire network.

Session Hijacking

Session Hijacking attacks are similar in nature to Man-in-the-Middle, except that the attacker will not directly forward traffic from the victim machine to its intended destination. Instead, the attacker will capture a genuine TCP sequence number or web cookie from the victim and use it to assume the victim’s identity. This could be used, for instance, to access a target user’s social media account if they happen to be logged in.

What is the Aim of An ARP Poisoning Attack?

Hackers have a wide [variety of motives](#), 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.

[Insider attacks](#) are of particular concern when thinking about ARP Poisoning. Spoofed ARP messages won't reach beyond the boundaries of a local network, so the attack must originate from a device that is locally connected. It's not impossible for an outsider to initiate an ARP attack, but they would need to remotely compromise a local system through other means first. An insider, meanwhile, would only need network access and some easily available tools.

ARP Spoofing vs ARP Poisoning



The terms ARP Spoofing and ARP Poisoning are generally used interchangeably. Technically, spoofing refers to an attacker impersonating another machine's MAC address, while poisoning denotes the act of corrupting the ARP tables on one or more victim machines. In practice, however, these are both sub-elements of the same attack, and in general parlance, both terms are used to refer to the attack as a whole. Other similar terms might include ARP cache poisoning or ARP table corruption.

What are the Effects of an ARP Poisoning Attack?

The most direct impact of an ARP Poisoning attack is that traffic destined for one or more hosts on the local network will instead be steered to a destination of the attacker's choosing. Exactly what effect this will have depends on the specifics of the attack. The traffic could be sent to the attacker's machine or sent to a nonexistent location. In the first instance, there may be no observable effect, while the second may inhibit access to the network.

ARP cache poisoning itself won't have a lasting impact. ARP entries are cached anywhere from a few minutes on end devices to several hours for switches. As soon as an attacker stops actively poisoning the tables, the corrupted entries will simply age out and proper flow of traffic will soon resume. ARP Poisoning on its own will not leave a permanent infection or foothold on victim machines. However, hackers often chain many types of attacks together, and ARP poisoning may be used in part of a larger campaign.

How to Detect an ARP Cache Poisoning Attack

```
Microsoft Windows [Version 10.0.19041.388]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\User A>arp -a

Interface: 172.16.55.5 --- 0x14
Internet Address      Physical Address      Type
172.16.55.1           7a-4f-43-36-82-65    dynamic
172.16.55.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\User A>
```

A variety of commercial and open-source software exists to detect ARP cache poisoning, but you can easily check the ARP tables on your own computer without installing anything. On most Windows, Mac, and Linux systems, issuing the “arp -a” command from a terminal or command line will display the current IP-to-MAC address mappings of the machine.

Tools like arpwatch and X-ARP are useful for continuous monitoring of the network and can alert an administrator if signs of an ARP Cache Poisoning Attack are seen. However, false positives are a concern and can create a large number of unwanted alerts.

How to Prevent ARP Poisoning Attacks

×

ARP Poisoning Prevention Tips:

- Static ARP tables
- Switch security
- Physical security
- Network isolation
- Encryption



 VARONIS

There are several approaches to preventing ARP Poisoning attacks:

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.

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.

DAI and similar features were once exclusive to high-end networking gear, but are now common on almost all business-grade switches, including those found in smaller businesses. It's generally considered a best practice to enable DAI on all ports except those connected to other switches. The feature does not introduce a significant performance impact but may need to be enabled in conjunction with other features like DHCP Snooping.

Enabling Port Security on a switch can also help mitigate ARP Cache Poisoning attacks. Port Security can be configured to allow only a single MAC address on a switch port, depriving an attacker the chance to maliciously assume multiple network identities.

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.

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.

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.

Just one of many threats

While it's been around far longer than modern threats like [Ransomware](#), ARP Poisoning is still a threat that organizations need to address. Like all cyberthreats, it is best addressed through a comprehensive information security program. A solution like the Varonis Threat Detection and Response can help you get an idea of your organization's overall security posture. [Varonis Edge](#) can help spot signs of data exfiltration that may occur after an ARP Poisoning attack has taken place.