veracode.com

ARP Spoofing

4-5 minutes

What Is ARP Spoofing?

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

ARP Spoofing Attacks

The effects of ARP spoofing attacks can have serious implications for enterprises. In their most basic application, ARP spoofing attacks are used to steal sensitive information. Beyond this, ARP spoofing attacks are often used to facilitate other attacks such as:

- Denial-of-service attacks: DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.

- Session hijacking: Session hijacking attacks can use ARP spoofing to steal session IDs, granting attackers access to private systems and data.
- Man-in-the-middle attacks: MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims.

ARP Spoofing Tutorial

ARP spoofing attacks typically follow a similar progression. The steps to an ARP spoofing attack usually include:

1. The attacker opens an ARP spoofing tool and sets the tool's IP address to match the IP subnet of a target. Examples of popular ARP spoofing software include Arpspoof, Cain & Abel, Arpoison and Ettercap.
2. The attacker uses the ARP spoofing tool to scan for the IP and MAC addresses of hosts in the target's subnet.
3. The attacker chooses its target and begins sending ARP packets across the LAN that contain the attacker's MAC address and the target's IP address.
4. As other hosts on the LAN cache the spoofed ARP packets, data that those hosts send to the victim will go to the attacker instead. From here, the attacker can steal data or launch a more sophisticated follow-up attack.

ARP Spoofing Detection, Prevention and Protection

The following methods are recommended measures for detecting, preventing and protecting against ARP spoofing attacks:

- Packet filtering: Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in ARP spoofing prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).
- Avoid trust relationships: Organizations should develop protocols that rely on trust relationships as little as possible. Trust relationships rely only on IP addresses for authentication, making it significantly easier for attackers to run ARP spoofing attacks when they are in place.
- Use ARP spoofing detection software: There are many programs available that help organizations detect ARP spoofing attacks. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.
- Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster ARP spoofing attack prevention by encrypting data prior to transmission and authenticating data when it is received.

Click here to learn how we can help strengthen web application security and protect applications from attack.