

Forum:[Hack Forums](#)

Thread: [What is ARP Poisoning](#)

K1. - March 13, 2021, 6:20 am

What exactly is ARP Poisoning?

ARP is an acronym. It stands for Address Resolution Protocol. What it does is convert an IP address to physical addresses a.k.a Mac Addresses on a networks switch. The host machine sends an "ARP" broadcast out on the network, and the recipient machine will respond with its own Mac address. The resolved IP/MAC address which has been acquired is then used to communicate across the network. ARP poisoning is all about exploitign the network and sending fake Mac addresses to the networks switch so that it can partner the fake Mac addresses with the IP address of the legit computer on a network and then in turn hijack the traffic using imitation.

What are ARP Poisoning Countermeasures

Static ARP entries: this is a good countermeasure and these can be defined in the local ARP cache on the network and then the switch is then configured to ignore all of the auto ARP response packets. The downside of this method is, it can be super hard maintain on bigger networks. IP/MAC address maps have to be distributed to all the computers on the network which make it a huge task for a large network.

ARP poisoning detection: some software systems can be used to cross reference the IP/MAC address resolution and certify that they are who they claim to be if they are authenticated. Uncertified IP/MAC address resolutions can then be dumped and blocked.

Operating System Security: this countermeasure is dependent on the operating systems which are being used. The following list are the basic techniques used by various operating systems to block this issue.

Linux based: these function by ignoring the unsolicited ARP response packets.

Microsoft Windows: the ARP cache behavior can be configured at the registry level. Here is some software which can be used to prevent such attacks:

AntiARP– provides full protection against both passive and active network sniffing

Agnitum Outpost Firewall–provides protection against only passive sniffing

XArp– provides some protection against all types, both passive and active sniffing