Report “ARP poisoning”

ARP (Address Resolution Protocol) Poisoning, also known as ARP Spoofing, is a man-in-the-middle (MITM) attack in which an attacker sends spoofed ARP messages over the local area network (LAN). This tricks devices on the network into sending data to the attacker rather than the legitimate recipient, allowing the attacker to intercept, modify, or block network traffic.

Vulnerable System:
OS
-Windows
-Linux
-MacOS
-Unix

HW
-Router
-Switch
-Access Point

This type of attack is current and capable of hitting many targets.

Risk & Mitigation

Risk
The risk with ARP poisoning is very high in network environments where switches are used. In this case the attacker "bombards" the entire network with ARP requests, managing to sniff the data traveling in it.

Mitigation

-Static ARP entries:

Ensures that devices always know who they’re talking to, preventing the bad guy from pretending to be someone else.

Works well for small networks but can be a headache to manage if you have many devices.

-Dynamic ARP Inspection (DAI):

A security feature available on many advanced switches. Validates ARP packets and ensures they come from trusted sources by cross-referencing DHCP snooping binding tables.

Requires compatible hardware and proper configuration.

-DHCP Snooping:

Monitors DHCP traffic to build a database of trusted IP-MAC pairsand helps to prevent unauthorized devices from receiving network access.

Needs to be configured on all switches to be effective.

-Segmentation and VLANs:

Use VLANs to segment the network and limit broadcast domains reduces the scope of ARP spoofing attacks to a single VLAN. Consider that requires proper network design and configuration.

-IPv6 Transition:

Transition to IPv6, which uses Neighbor Discovery Protocol (NDP) instead of ARP. NDP includes Secure Neighbor Discovery (SEND), which is more secure against spoofing.

Consider that requires network infrastructure that supports IPv6.

COSTS:

The cost of mitigating ARP spoofing can vary based on the complexity of the network and the size of the organization. Implementing static ARP entries is a low-cost option, primarily involving the effort of IT staff without the need for significant hardware or software purchases.
Detection and prevention solutions, such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) like Snort, represent a medium-cost option. These systems require an initial investment for the software and potential hardware upgrades, with an estimated cost between 1,000€ and 5,000€.
For enhanced security, network segmentation using VLANs is an effective solution. Although it requires a higher initial expenditure for configuring and managing VLANs, with costs estimated between 2,000€ and 10,000€, this option ensures a more secure and organized network. Network Access Control (NAC) solutions, such as Cisco ISE, offer comprehensive control over network access. These solutions represent the most expensive option, with investments ranging from 10,000€ to 50,000€, but they provide extensive protection against a wide range of network threats. Finally, adopting dedicated anti-ARP spoofing software, such as ArpON, presents a variable-cost solution. Purchasing and implementing such software can cost between 500€ and 5,000€, depending on the specific needs of the corporate network.

In conclusion..

Implementing ARP spoofing mitigation measures is crucial for several reasons. First, it protects sensitive data from unauthorized interception and modification, safeguarding critical information such as intellectual property, customer data, and financial information.
Moreover, it ensures the integrity of the corporate network by preventing significant service disruptions that could compromise the company's reputation. ARP spoofing attacks can cause downtime and loss of productivity, making operational continuity a top priority.
Adopting these measures is also essential for maintaining compliance with data security regulations such as GDPR and HIPAA, which require the implementation of adequate security measures to prevent cyber attacks. ARP spoofing mitigation helps meet these regulatory requirements.
Finally, it reduces the risk of more severe attacks. ARP poisoning can serve as a gateway to more complex attacks such as man-in-the-middle (MitM), DNS spoofing, and session hijacking. Preventing these attacks strengthens the overall security of the network.

As part of our ongoing commitment to the security and integrity of corporate data, it is crucial to implement measures to mitigate ARP spoofing. This type of attack poses a significant threat to our network, potentially leading to data loss, service disruption, and damage to our reputation.
Investing in ARP spoofing mitigation is not just about protecting our data and network but also a fundamental step to ensure regulatory compliance and reduce the risks associated with more severe attacks. The proposed solutions vary in cost, but the benefits far outweigh the necessary investments.
We encourage you to favorably consider allocating the funds required for these essential security measures. Protecting our data and ensuring operational continuity are vital for the long-term success of our company.