
Detect ARP poisoning(ARP spoofing) & ARP flooding

Posted by Devid Huang - 2009/02/15 03:45

Address Resolution Protocol (ARP), because of its simpleness, fastness, and effectiveness, is becoming increasingly popular among internet rappers, thus causing severe influence to the internet environment.

ARP spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network which may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether (known as a denial of service attack). The attack can obviously only happen on networks that indeed make use of ARP and not another method.

With Ax3soft Sax2, we can quickly and accurately locate ARP source when ARP attack happens to the network, so as to ensure normal and reliable network operation.

Solution:

Diagnosis View is the most direct and effective place to locate ARP attack and should be our first choice. Its interface is displayed as picture1.

<http://www.ids-sax2.com/articles/images/QuickLocateARPAttackSource.gif>

(picture1)

Picture 1 definitely points out that there are two kinds of ARP attack event, ARP Scan and ARP MAC address changed, in the network, and the attack source is clearly given at the bottom. Meanwhile, Sax2 NIDS will provide reasons of such ARP attacks and corresponding solutions.

=====