Detection and Prevention of ARP-Spoofing Attacks

Gunjan Agrawal
VIT Chennai

***Abstract* - The ARP protocol is used extensively in internet for mapping of IP and corresponding MAC address. Since it suffers from lack of authentication, it is prone to a spoofing attack often known as "ARP spoofing attack". This spoofing can then further lead to Man-in-the-Middle Attack, DoS attack, etc. This paper proposes a few methods to detect and prevent ARP spoofing.**

INTRODUCTION

Most of the organizations implement LAN for their communication and networking needs. In LANs, the identifier used for communication is MAC address. Thus transfer of packets require resolving IP address to MAC address for communication within a LAN. This resolution is done by the Address Resolution Protocol (ARP).
However, this protocol suffers a major security issue. ARP protocol is stateless. It does not authenticate whether any request was made for the response received. Thus it becomes prone to an attack known as ARP spoofing attack or ARP cache poisoning.
This paper proposes methods to detect and to prevent or mitigate ARP spoofing.

DETECTION OF ARP SPOOFING

Lets first understand how ARP spoofing is done.
The PC 'V' in the given figure represents the victim's PC, the router is represented by 'R', the attacker is represented by 'A'.

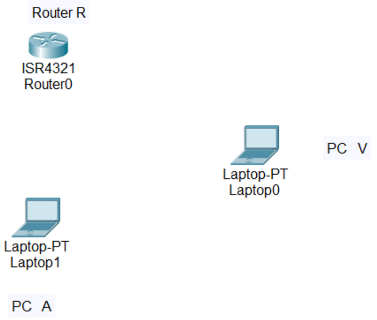

Fig.1 showing A, V and R

A sends spoofed ARP packet to V claiming that A is the router.
B without any authentication, records this entry into its ARP table and assumes that A is the router.
A sends spoofed ARP packet to R claiming that A is V (while actually its not)
R without any authentication, records this entry into its ARP table and assumes that A is V.
So, the actual path of packet transmission now becomes (see the figure below)

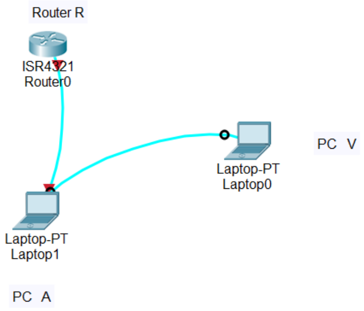

Fig.2 showing the new path for communication formed due to spoofing

Now the entire communication between R and V is passing through A. This is the case of a typical Man-in-middle attack. A can now modify, drop or view entire data transmitted or received by V.
The attack can be identified by 2 entries in the ARP table of V. The ARP table of V will contain two entries, these two entries will have different IP addresses but the same MAC addresses.
The first entry will correspond to the authentic entry. By authentic entry I mean that the first entry in the table will correspond to the MAC and IP address of R.
The second entry will correspond to the IP address and MAC address (spoofed, same as that of R) of A.

PREVENTION OF ATTACK

The following text describes the proposed methods that can be used to prevent such attacks.

Method 1: Use of static IP addresses

The organization owning the network has to ensure that static IP addresses are being used in the network.

As we discussed above, in case of ARP spoofing, two entries will correspond the same MAC address. We know that the first entry corresponds to the gateway/router. Hence, we have to block the communication with the IP address corresponding to the second entry. The second entry corresponds to the entry made by the spoofed packet.

So, we can simply block the communication with IP address corresponding to the second entry.

Method 2: Designing a new protocol

We design a new protocol in which any host has to flood a probe packet across network as soon as it detects an entry into its ARP table.

The probe packet will contain the MAC and IP address pairs of the source and destination.

Whenever any host receives this probe packet, it has to send an acknowledgement saying IP address is matched or MAC address is matched. Reply has to be sent separately corresponding to the correct matching of IP address and MAC address.

In case of a mismatch, the destination will simply won’t reply to the sender.

Hence, in case of an authentic connection, the sender will receive two responses from a single destination. One response will correspond to the correct matching of IP address and the second response will correspond to the correct matching of MAC address.

Now in case of ARP spoofing, the sender will receive unequal number of replies for MAC and IP addresses. The reason for this is as follows:

Corresponding to the first entry (which is authentic), the sender will receive 2 replies. One saying that IP address is matched and other saying that MAC address is matched.

Now in case of the second entry(which is spoofed), the sender will get reply corresponding to matching of correct IP address but he won’t get reply corresponding to correct matching of MAC address. This is because, the attacker has not changed the MAC address of the NIC card physically, he has artificially created packets with wrong MAC address and injected them into the network.

Thus if everything is fare and fine, the sender will get equal number of replies for both IP and MAC address matching. If some spoofing happens, then the sender will get unequal number of replies.

Now we can block communication with that IP address for which the sender didn’t receive the reply corresponding to the MAC address.

Method 3: Use of softwares

The organization can consider deploying some specific software into each and every system of their organization. These softwares will ensure that programs that can spoof IP addresses can’t be run or installed on the systems. Furthermore, a server can keep a check that all systems in the network have these programs installed.

Thus if an attacker intrudes into the network, he won’t have this software installed.

For example, Technitium is a software that can change MAC address of the system. So we can design and deploy software that can detect software or scripts like Technitium and block them.

The server can simply prevent the devices which do not have this software installed from communicating over the network.

SUMMARY

In this paper, we proposed techniques to detect and prevent ARP spoofing. These techniques might have few loopholes or drawbacks. These techniques can be easily deployed within a LAN.

Method 1 is the most effective, Method 2 requires a new protocol to be designed and Method 3 is expensive and cumbersome due to deployment of software or server.

Any of these methods can be deployed depending upon the requirements of the organization.

REFERENCES

[1] “Data Communications and Networking” by Behrouz A. Forouzan, McGraw Hill, Fifth edition

[2] Poonam Pandey , “Prevention of ARP spoofing: A probe packet based technique”, 2013 3rd IEEE International Advance Computing Conference (IACC)