Arp Spoofing Detection -- An Active Technique

Vivek Ramachandran , vivekr@iitg.ernet.in
Indian Institute Of Technology , Guwahati

ABSTRACT :

Arp spoofing is one of the most commonly used technique by an attacker to compromise security of a LAN . This is also sometimes the starting point For more sophisticated attacks such as Sniffing ,Denial Of Service, Man In The Middle etc . In this paper I have proposed an active method to detect Such a "Spoofing" . The detection is done almost instantaneously .

BACKGROUND :

Most commonly used tools today use a passive approach to ARP spoofing detection By just monitoring the network traffic and report any flips which might occur. Note that this method will only detect spoofing when two contradicting ARP messages are received . So there is a waiting period till a detection occurs . As most ARP spoofing tools periodically send ARP cache refresh messages hence there might be no need for the victim hosts to send any requests or replies , thus increasing the time of detection . Also if a non exsistent host is used in the spoofing then the flip may never occur at all , thus making it impossible to detect the threat . The passive tool will just add this as a new entry in it's table .

ATTACK SCENARIO :

The discussion in this paper will be based on the following topology , which is also the basic building block of any ARP based attack :

Terminology :

SpoofDetect : Our Spoof detection software .

IDS : The admin PC running SpoofDetect .

A : Attacker's PC .

V1 : Victim 1 , whose ARP reply **A** forges .

V2 : Victim 2 , to whom **A** sends the forged reply .

In the most basic of attacks let us suppose that **A** sends a spoofed reply to **V2** from **V1** .

ARP reply : **V1** ------> **V2**

DETECTION METHOD :

My method takes into account the fact that the attacker cannot stop the victims from responding to other ARP requests from the connected network .

SpoofDetect maintains a database of correct entries , which are decided by the following algorithm : --

1. Sniff for ARP replies . As soon as you receive an ARP reply , check the database if any entry exists corresponding to **V1** & **V2** , if yes then check if the IP to Hardware (HW) mapping matches or not .

2. If a correct match occurs from the database then the hosts are legitimate else if there is a change then spoofing is going on (assuming no IP conflicts between hosts) .

3. If there is no entry corresponding to **V1** or **V2** or both then send ARP request from **IDS** to them .

4. Now check the replies from **V1** and **V2** to **IDS** with the entries sent to each other . If they match then no spoofing , if they don't then there is spoofing .

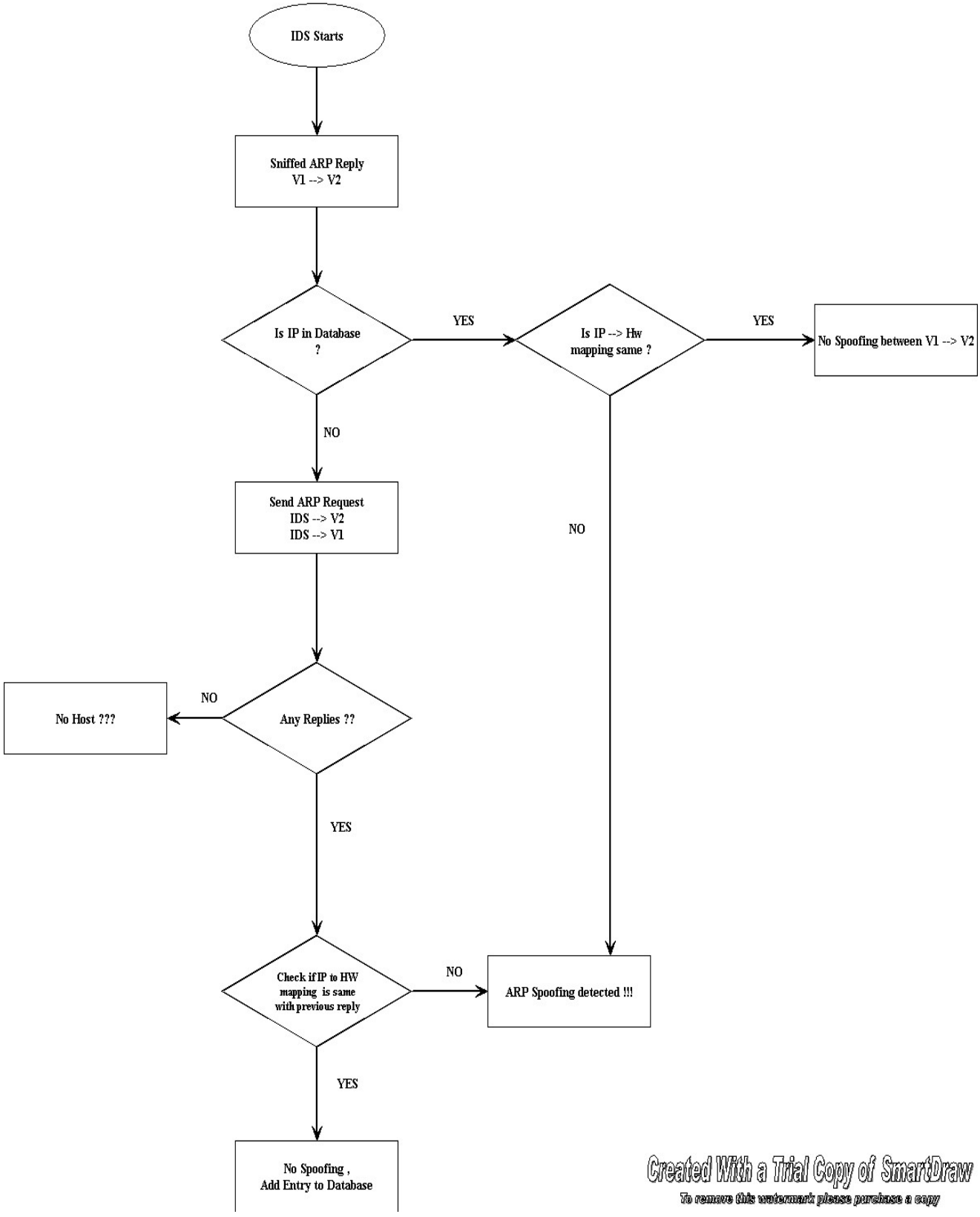
5. If **A** is also replying to other hosts (smart one) , then IDS would at least receive a duplicate reply (one from real host + one from **A**) .

6. In either case there will be a mismatch between the 2 entries thus spoofing detected !!!

7. Also if we consider an ARP flood attack (say a switch ARP cache overflow attack) , then when IDS sends ARP requests to **V1** then it will not receive any replies , thus detecting the possible case of a "fake host" .

The flowchart below shows the above algorithm in a graphical format :

Active Method for ARP Spoofing detection - Vivek Ramachandran



Discussions :

Network Overhead :

A active tool always adds an extra load on the network , but this algorithm ensures that for every "existing host" on the network only one ARP reply will be sent from **IDS** . After a successful addition of a host any ARP reply from it would only involve a comparison from the database built by **SpoofDetect** .

Though this tool will successfully detect a "fake host" attack (ARP replies from non existent hosts being sent) , note that a flood of such packets will result in a flood of requests from **IDS** . Thus for a successful implementation an upper threshold should be kept for the no of requests sent and correspondingly no replies received .

ADVANTAGES :

The main advantage is the speed of such a detection compared to passive tools which wait for a mismatching reply . Also note that a "fake host" attack may never be detected by a passive tools as no mismatch will ever occur in such an attack .

FAILIURES :

If the attacker is impersonating a "fake host" and sends ARP replies to all ARP requests then this method fails , as when **IDS** sends it's ARP request to say **V1** (fake host) , then **V1** replies to **IDS** with same fake credentials . though if the administrator adds a database of valid IP addresses to increase the knowledge of **IDS** of the network topology then , this attack will be detected .

TOOL :

The tool SpoofDetect has already been coded by me and has been successfully, tested . I will soon be releasing the tool online .