A New Approach to Prevent ARP Spoofing

Divya Sharma, Oves Khan, Kanika Aggarwal, Preeti Vaidya

Abstract— Many intra-domain protocols (like IP, ARP) do not have protection against malicious activities by network users. As a result IP and ARP spoofing are used by attackers to launch Man in the Middle (MITM), Denial of Service (DoS) and other attacks. These attacks are severe threats to the network users. Detecting and preventing IP-ARP spoofing will enhance the security to great extent. This paper presents a simple mechanism for detection and prevention of IP-ARP spoofing.

Index Terms—ARP Spoofing, IP Spoofing, Spoofing Detection and prevention.

I. INTRODUCTION

The ARP protocol belongs to the family of IP/TCP protocols that . For this purpose, an ARP table is constructed which maps the MAC address for every IP address. When a request is made for a packet to be delivered, ARP first consults the table to determine if the MAC address for the destination IP address had already being determined. Thus, the table helps in speeding up the response to the request. If no entry is found corresponding to the IP address in the table, then the MAC address is determined by the protocol, and the ARP table is updated.

By default, most of the entries in the ARP table are dynamic in nature. This allows the system to be flexible. For example, if a machine accesses the network with a different IP address than that already stored in the ARP table, or if a network is reconfigured, then the dynamic nature of ARP table allows correct MAC addresses to be updated corresponding to their IP addresses.

However, this nature of ARP tables can be exploited by crackers for spoofing attacks, including Man in the Middle Attack and Denial of Service. A popular tool for this purpose is NetCut.

The rest of this paper is organized as follows. Section 2 gives introduction of IP Spoofing based attacks. Section 3 gives brief introduction of ARP Spoofing-based attacks. Section 4 gives details about the recent work done Section 5 gives overview of proposed work done for detection and prevention of IP and ARP spoofing based attacks. Section 6 presents the experimental results. Section 7 concludes the paper..

II. IP SPOOFING BASED ATTACKS

A. Review Stage

IP Protocol: Internet Protocol is basic and most widely used connectionless protocol in TCP/IP suit. It is used to represent a host on the network.

Revised Manuscript Received on June 06, 2013.

Ms .Divya Sharma, CSE Department, ITM University, Gurgaon, India.
Mr. Oves Khan, CSE Department, ITM University, Gurgaon, India.
Ms. Kanika Aggarwal, CSE Department, ITM University, Gurgaon, India.
Ms.Preeti Vaidya, CSE Department, ITM University, Gurgaon, India.

IP Spoofing: IP spoofing is process of forging the Source IP addresses in TCP/IP packets. It is one of the widely used mechanisms by hackers to launch DDoS attacks.

Types of IP Spoofing-based attacks: Connectionless nature of IP protocol is exploited by attackers to launch following attacks.

B. DoS Attacks

Large volume of Spoofed IP packets are sent to a target host or server. This high volume of traffic makes that machine unable to respond to a genuine traffic. Since attacker is not interested in response to these spoofed packets, IP spoofing is most suitable for such attacks.

C. DDoS Attacks

Huge volume of Spoofed IP packets are sent to a target host or server from many machines. This method is used to make DoS attack detection Security systems less effective.

III. ARP SPOOFING BASED ATTACKS

A. ARP Protocol [1]

If The Address Resolution Protocol (ARP) [2] is used to map IP address to MAC address. This protocol plays an important role in LAN environment, as each frame transmitted by host must contain a destination MAC address. If IP address of a destination host is known, then ARP is used to determine the host's MAC address. This MAC address is then used to deliver frames to destination host on the network. The working of ARP protocol is as follows

1) The host broadcasts an ARP request message on the network to determine MAC address of another host.
2) All the hosts connected to LAN receive the request.
3) The host, whose IP address matches with the destination IP of ARP request message, sends back a unicast ARP reply containing its own MAC address.
4) After receiving ARP reply, the host caches the (IP, MAC) pairing in a local ARP cache to avoid the same ARP request in future.

B. ARP Spoofing

ARP spoofing is a process of creating and injecting fake ARP entry and ARP messages on the network. It is used by the attackers to control the flow of packets over a network according to their requirement.

C. ARP Cache Poisoning

ARP [2] is a stateless protocol. Even though ARP request is not issued by host and it receives an ARP reply message, it will update its own ARP cache using ARP reply message. Attacker takes advantage of this by using ARP Spoofing to manipulate the ARP cache of target host(s). This manipulated ARP cache is then used to launch Man-In-The-Middle (MITM) and DoS attacks. This process of manipulating the ARP cache

for malicious activities is called as ARP cache poisoning.

IV. RELATED WORK

In [3], detection of MAC spoofing attacks is detected by sending a request of Inverse ARP for a MAC address. The received response can be used to determine whether computer is performing cloning [4].But this solution is very limited as it only detects this type of ARP attacks.

By port security [5], cloning attacks can be prevented. This method is effective but it fails in other type of ARP attacks which does not require cloning of MAC address [4].

Tripunitara et al. [6] discussed about a middleware approach to asynchronous as well as for backward compatible detection and prevention of ARP cache poisoning attacks. But this scheme is not effective if host being spoofed is down or being DOSed.

Neminath H.el at [7] proposed a light weight mechanism by using static transition tables for detection of ARP response spoofing bit it does not provide any solution against the attack. Wenjian Xing et al [8] proposed a defense mechanism against ARP attacks which is based on the inspection of ARP packets by using RAW socket programming.

Masurai[9] uses static IP-MAC pair entries for every host on the network. System administrator maintaining these entries but this kind of network fails for large organization.

D.Bruchi et al [10] proposed a new Secure-ARP (SARP) protocol in which key distribution, public and private keys for signing every ARP message have been used. Separate server has been for resolving AP request based on secrete sharing concept.

V. PROPOSED WORK

In this proposed work we are preventing ARP spoofing by using static ARP entry in ARP table in place of dynamic entry which by default provided to the user.

Following are the steps we are going to follow ARP spoofing ,the ARP table is flooded by another entry of MAC address corresponding to the same IP address the packets which were to deliver to original MAC address now begin to distract their path to fake MAC address generated by the hacker

To prevent this we implement a the corresponding technique, As the MAC address is dynamic so the hacker could easily change the physical address by using ARP spoofing softwares

In order to make networking ARP Spoofing proof we use static entries in the ARP table and make the MAC address static this makes the entries constant and the hacker would now won't be able to apply ARP spoofing in the network the static entry is done using windows command prompt like ARP -sip_addressmac_address.

VI. EXPERIMENTING DETAILS

The Using windows command prompt we generated ARP table and monitor the network then by using the software netcut we tried to spoof the network by sending false ARP entry in the ARP table the entry so generated now prevents the PC to access the internet as the packets are now being deliver to the false MAC address generated by the hacker ,we then modified the ARP table corresponding to the our Internet Protocol address and assign it to the MAC address of the machine of which the packets are to deliver ,now the packets are delivering to the PC we wanted and the network is up and running again.

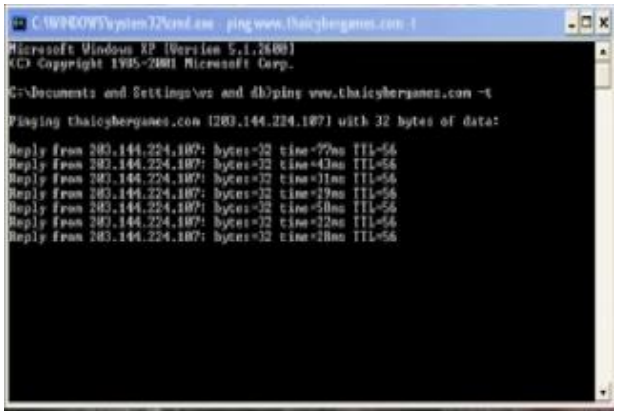

Fig. 1.Testing of Network

In Fig. 1 the network was tested and found the internet connection is up and running this was accomplished with the windows command prompt

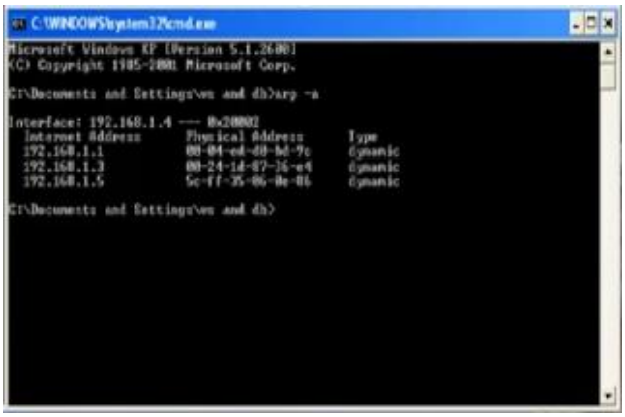

Fig. 2 ARP Table

In Fig. 2 the ARP table was viewed using windows command prompt using the command 'arp –a' the command on successful execution showed ARP table in which MAC address corresponding to the IP entries and found that the MAC corresponding to the IP address is dynamic and prone to ARP Spoofing attack.

Fig. 3 Attack on PC

In Fig. 3 software netcut is used to attack the victim's PC and perform the above operation by ARP Spoofing it changes the victim's MAC address corresponding to the IP address

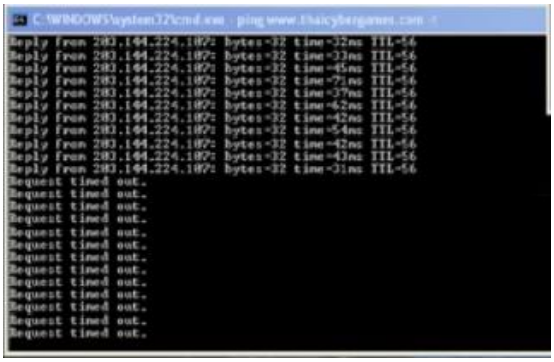

Fig. 4 Spoofing of Network

In Fig. 4 when hacker spoofed the network the packets that were to receive by the victim's PC now began to travel to the false MAC address corresponding to victim's IP address because of ARP spoofing and the internet access is cut.

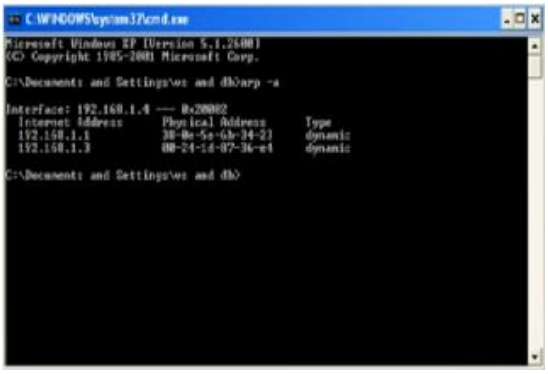

Fig. 5 Manipulated MAC Entries

Comparing these two figures, Fig. 2 and Fig.5. The Fig. 2 is the figure representing the original MAC address corresponding to the victim's IP address while the Fig. 5 represents the manipulated MAC entry in ARP table and hence the victim's Pc is ARP spoofed.

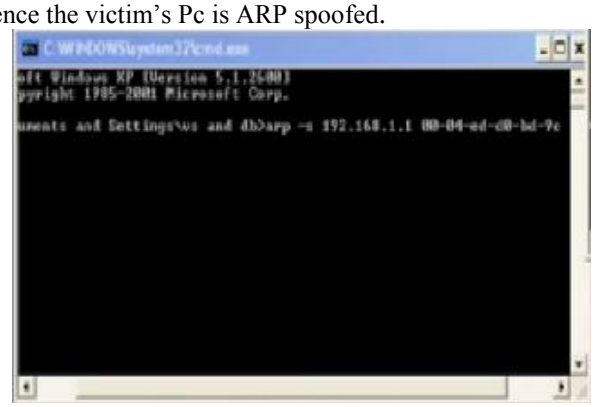

Fig. 6 Static Entry

In Fig. 6 the static entry is made corresponding to the victim's IP address.

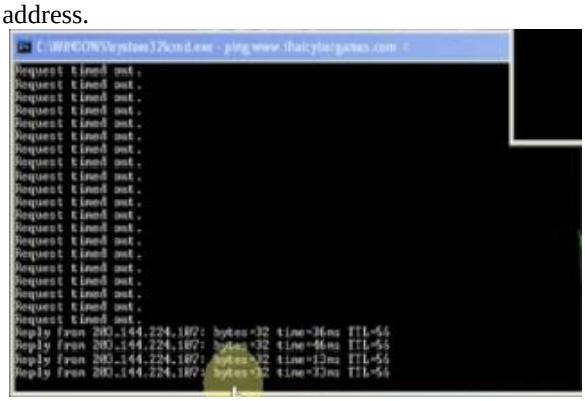

Fig. 7 Prevention of Spoofing

On making the static entry the reply began to come and the ARP spoofing is prevented.

VII. CONCLUSION

The proposed mechanism for IP and ARP spoofing detection has following plus points:

1) Can block attack at the surce of attack itself.
2) It can prevent IP and ARP spoofing based attacks.

REFERENCES

1. David C. Plummer, "An Ethernet Address Resolution Protocol", Request For Comments: 826
2. S.J. Bhirud, V. Katker, "Light weight Approach for IP-ARP Spoofing Detection and Prevention",In Proc. Second Asian Himalyas International Conference on Internet,pp. 1–5, Nov 2011.
3. T. Bradley, C. Brown, and A. Malis. Inverse address resolution protocol.RFC 2390, September 1998.
4. S. Whalen. An introduction to arp spoofing.2600: The Hacker Quarterly,18(3), Fall 2001.
5. http://www.node99.org/projects/arpspoof/arpspoof.pdf.
6. C. Schluting. Configure your catalyst for a more secure layer 2, January 2005.http://www.enterprisenetworkingplanet.com/netsecur/article.php/3462211.
7. M. V. Tripunitara and P. Dutta," A middleware approach to asynchronousand backward compatible detection and prevention of arp Cache poisoning",In Proc. 15th Annual Computer Security Application Conference(ACSAC), pages 303–309, 1999.
8. Neminath H, S Biswas, S Roopa, R Ratti, R Nandi,FA Barbhuiya, A Sur, V Ramachandran, "A DES Approach to Intrusion Detection System foe ARP Spoofing Attacks", 18th Mediterranean Conference onControl & Automation (MED), ISBN: 978-1-4244-8091-3, IEEE 2010.
9. Wenjian Xing, Yunlan Zhao, Tonglei Li, "Research on the defense against ARP Spoofing Attacks based on Winpcap", 2010 Second International Workshop on Education Technology and Computer Science, Digital Object Identifier: 1O.l109IETCS.201O.75, 2010 IEEE.
10. Somnuk Puangpronpitag, Narongrit Masusai, "An Efficient and Feasible Solution to ARP Spoof Problem", 6th International Conference on Electrical Engineering lElectronics, Computer,Telecommunications and Information Technology,2009. ECTI-CON 2009. ISBN: 978-1-4244-3387-2.
11. D. Bruschi, A. Omaghi, E. Rosti, "S-ARP: a secure address resolution protocol, "Annual Computer Security Applications Conference (ACSAC), 2003.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication