© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Various Prevention mechanism for ARP poisoning against MITM attack

Dhrruv Chaudhary[1], Jahnavi Vithalpura[2]
[1]ME Student, Information Technology Department LD College of Engineering, Ahmedabad, Gujarat, India
[2]Assistant Professor, Information Technology Department LD College of Engineering, Ahmedabad, Gujarat, *India*

ABSTRACT

The address resolution protocol (ARP) is a protocol that is used by the IP. The ARP works inside the switches and is used for mapping of the IP address and MAC address. ARP works properly but it is a stateless protocol therefore it can be easily attacked. That because hacker can perform MITM on the network and easily still the information which is communicate between two hosts of network. Our project provides a lightweight approach for detecting such attacks is to use Snort. Snort is intrusion detection system (IDS). It will alert us on attack and will use the Open source interface to get the IP address of the attacker/hacker and for preventing we will block it by scripting based on python programing language. After blocking IP of hackers he will not capable to perform MITM on the network again and provide accurate result.
Keywords : Virtualization, Attacks, Network Security, ARP Poisoning, Man in the Middle Attack

I. INTRODUCTION

Today internet has become the basic necessity for most of the people and in last few years its growth has significantly increased. So to use internet there are many types of network by which people have access to the internet like wired network and wireless networks. In wireless network we can include Wi-Fi, Wi-Max, Bluetooth, etc. And for securing these types of network there are multiple approaches are there. But every approach has challenges which need to be addressed. So one of the protocol used is the Address Resolution Protocol (ARP). But there are some cons of ARP. One of them is its stateless nature. And for ARP, ARP Poisoning attack is used to disrupt the functions of it in switched network. And by doing ARP Poisoning, Man in the Middle (MITM) attack is also possible. So there should be standard mechanism from protection of ARP Poisoning attacks. In everyday environment, people think that it is not possible to eavesdrop the packet in switched network or in encrypted wireless (Wi-Fi). Because they think that switch is point to point device and computer will talk to specific endpoint of switch which it want to. But in today's life there are many hacking and penetration tools which can hack that system, which allows anyone running these type of tools to view all traffic flowing in network and they might change the traffic flowing in the network means performing the man-in-the-middle attack. So for this type of attacks there are solutions like Arp-Defender for defending and Arp-Watch for monitoring but these solutions are costly and also have disadvantages. Means there is the need for the single solution to preventing and detecting the ARP Poisoning attack.

ARP stand for "ADDRESS RESOLUTION PROTOCOL". ARP protocol works with internet protocol (IP) used for finding the connection between the two different hosts in a single network using their IP address and MAC address; where hosts are using ARP request/reply packet of ARP. By the ARP request packet sender host asks for the receiver using IP address of receiver host and after that receiver host gets request and replies with MAC address using ARP reply packet.

ARP protocol works between the network layer and data-link layer. The network layer provides IP address to the machine and by data-link layer MAC address to communicate. By using ARP protocol we can find how many hosts are connected in the network and also discovers hosts' IP address and MAC address.
ARP protocol using two packets:
1) ARP request packet
2) ARP reply packet

II. PROBLEM DEFINITION

After the ARP was drafted, a subtle weakness was found. Infect Arp does not provide the authentication to the source of incoming ARP packets this is the reason that an attacker can forge an ARP message containing malicious information to poison the ARP cache of the target host.

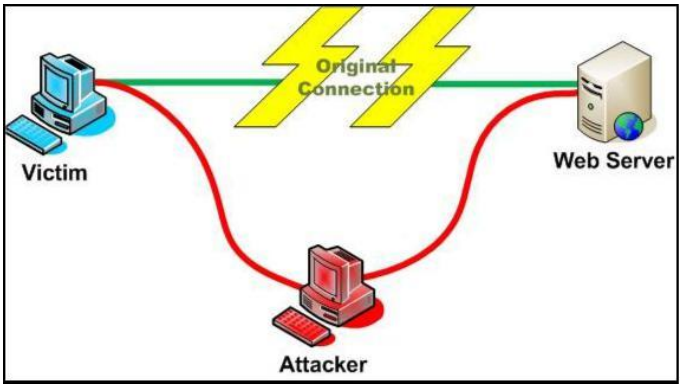

Figure 1. ARP Poisoning Attack

ARP suffers from the lot of threats which leads it to insecure communication and the lonely reason for these attacks is the no authentication mechanism is used in the ARP. When the victim adds an incorrect (IP, MAC) mapping to its ARP cache, this is known as the cache poisoning or Arp spoofing. The ARP poisoning is done when the attacker sends the fake <IP, MAC> address in the response of ARP request, The ARP is stateless protocol and it accepts all the incoming ARP packets and modifies the local ARP cache.ARP poisoning attacks are often used as a part other serious attacks or we can say Arp poisoning is the base for the various attacks:

A. MITM ATTACK

In MITM the attacker attacks two hosts at the same time by cache spoofing two hosts in the network, the attacker can silently sit between the two hosts and can read/ write the communication between two victims so that they think that they are communicating with each other, this attack is passive attack and is difficult to detect.

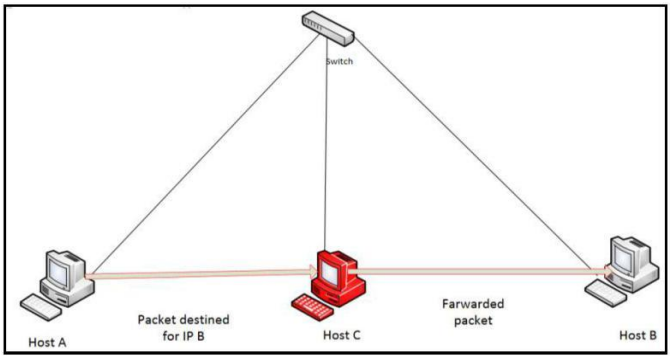

Figure 2. MitM Attack

B. ARP CACHE POISONING ATTACK

ARP protocol specifies no rules to maintain consistency between the ARP header and the Ethernet header [3]. That means one can provide uncorrelated addresses between these two headers. For example, the source MAC address in the Ethernet header can be different from the source MAC address in the ARP header. Moreover, ARP protocol deploys no mechanism to detect and prevent invalid association of IP and

MAC addresses proved in an ARP header. Hence, a malicious
host may exploit this weakness in the ARP protocol to introduce a spurious IP address to MAC address mapping (fake<IP-MAC> entry) in another host's ARP cache. This malicious act of creating fake ARP entries in an ARP cache is called ARP cache poisoning attack. The attack can be performed by directly manipulating the ARP cache of a target host, independently of the ARP messages sent by the target host. ARP cache poisoning attack is used usually to perform DoS or MitM attacks in network.

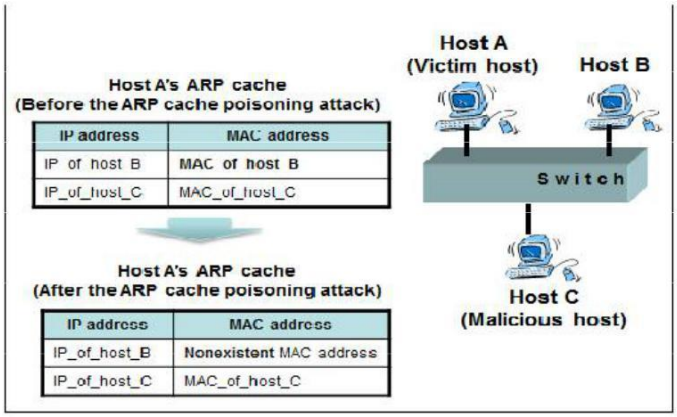

Figure 3. Host A's ARP cache before and after the ARP cache poisoning attack

III. A BRIEF REVIEW

Till present time there are many solutions for ARP-attacks to prevent the ARP-cache poisoning attacks and also provides the solution for security of ARP. Many researchers have done a good job and effort to prevent the attacks in ARP but these solutions have some drawbacks which cannot be tolerated by the network communication mechanism these solutions and their drawbacks.

A. USING STATIC ARP ENTRIES

Use of static ARP entries [1] is the best defence method for ARP cache poisoning attacks. We can make the MAC address static, hence it will make the entries constant and the hacker will not be capable to apply ARP spoofing in the network. This entry is done using windows command prompt like ARP-sip_addressmac_address. However this method is not suitable for big networks as it would be very complicated for the network administrator to manage and update these tables throughout the network.

B. S-ARP

A new Secure-ARP (S-ARP) [4] in which key distribution, public and private keys for signing every ARP message have been used. These keys are distributed by the trusted third party known as certification authority.

But this method has no backward compatibility means takes large cost and tough hard work to implement in the existing ARP.

C. DYNAMIC ARP INSPECTION

Some High-end Cisco switches presented a feature known as Dynamic ARP Inspection [6] that allows the switch to block invalid <IP, MAC> combinations. It uses local pairing table that is built using a feature recognized as DHCP snooping to detect which pairings are invalid. But the high costing of switches makes this feature ineffective.

D. ARP WATCH AND ARP GUARD

ARP watch [5] and ARP Guard [6] are the manual solutions that form an active protection against internal ARP attacks by constantly analyzing all the ARP messages, sending appropriate alerts in real time and identifying the source of attack.

E. MR-ARP

It is a non-cryptographic approach [13]. In MR-ARP if any new IP, MAC binding request comes then the genuineness of that request is checked by voting and if more than 50% reply comes into the favour of that binding then only the binding is accepted. If no reply will come then we consider this binding as genuine that's why any other node is not voting against the node and the binding will be accepted. This condition can be satisfied in the Ethernet, but may not be valid in the wireless LAN network because of the traffic rate adaptation based on the signal-to-noise ratio (SNR).

F. AVOIDING MAN IN THE MIDDLE ATTACK BASED ON ARP SPOOFING IN THE LAN

In this paper [17] they had trying to remove MITM specially ARP poisoning by using switch third party. Where third party encrypted the MAC address of host so attacker cannot interfere.

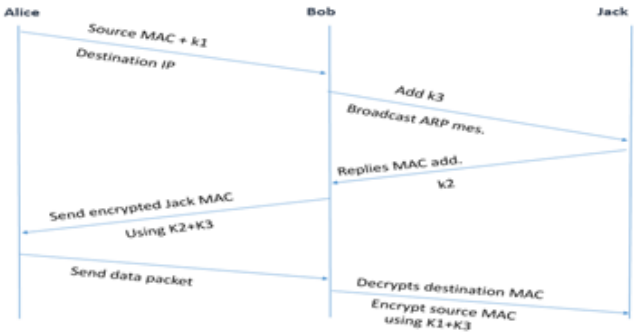

Figure 4. Encryption method

G. DETECTION AND PREVENTION AGAINST ARP POISONING ATTACK USING MODIFIED ICMP AND VOTING

In this paper [18] author used 4 machine for implementation of proposed mechanism. Central service node, 2 victim node and one attacker node are connected in wired network. Victim node maintain two tables, primary cache and secondary cache table and central service maintain only secondary table. In this paper author implemented three algorithm.

1) Client side implementation
2) CS side implementation
3) CS antidote implementation

F. DETECTION AND PREVENTION OF ARP POISONING IN DYNAMIC IP CONFIGURATION

In this paper [19] author defined prevention method for the system has three module.

1) DHCP IP configuration using DHCP Server
2) Authentication of the user using radius server + MySQL database
3) Detection and Prevention of ARP Poisoning.

IV. COMPARISION BETWEEN VARIOUS METHODS

Scheme	Method	Advantages / Disadvantages
Static Cache entries[1]	Use of static ARP cache entries.	Simple method but not appropriate for large networks.
S-ARP[4]	Signed ARP messages using public private keys.	Failure of third party leads to failure of whole network.
ARP Watch [5]	Monitors the traffic and generate alarms based on the rule.	Free but produce high number of alarms thus increasing work of admin.
ARP Guard [6]	Sniffing and generating alarms based on the rule.	Seems to be good but costly.
Dynamic Detection Approach based on Snort [7]	Sniffing and generating alarms based on the rules.	Free but increases the work of admin by generating high number of alarms.
MR - ARP [13]	Extended version of ARP to prevent attacks based on the concept of voting.	Might not be valid in 802.11 networks due to auto rate fallback.
Avoiding Man In The Middle Attack Based On Arp Spoofing In The LAN [17]	Remove MITM specially ARP poisoning by using switch third party. Where third party encrypted the MAC address of host so attacker cannot interfere	If third party fail whole network will be fail Used Encryption method every time need to encrypt.
Detection and Prevention against ARP Poisoning Attack Using Modified [18]	Implemented algorithms for each node and ICMP and voting technique	We have to implement each node and also require mathematic for polling score. O(log(n)), O(1)
Detection And Prevention Of ARP Poisoning In Dynamic IP Configuration [19]	DHCP IP configuration using DHCP Server Authentication of the user using radius server + MySQL database Detection and Prevention of ARP Poisoning.	Require Server Require Database for the Authentication

Table 1.1 Comparisons of Various ARP Prevention Methods

V. RESILIENCE AGAINST ARP CACHE POISONING

During an ARP cache poisoning attack, the malicious host can either create a new fake ARP entry in the target host's ARP cache or update an already-existing ARP entry using fake IP and/or MAC addresses proved in the ARP header of the ARP message. In principal, to corrupt an ARP entry, the malicious host may use a method based on generating either fake ARP reply messages or fake ARP request messages. These two methods are explained as follow:

ARP cache poisoning based on ARP reply messages: The malicious host may attempt to send fake ARP reply messages to a target host even though the malicious host did not receive any ARP request message from the target host. If the operating system deployed in the target host accepts any ARP reply message without checking whether or not an ARP request message was generated before, then the received ARP reply message can corrupt the target ARP entry or create a new fake ARP entry.

ARP cache poisoning based on ARP request messages: Alternatively, instead of sending fake ARP reply messages, the malicious host may attempt to send fake ARP request messages to corrupt the target ARP entries or create new fake ARP entries. In this case, when a target host receives a fake ARP request message, it believes that a connection is going to be performed, and then, updates the target ARP entry or creates a new ARP entry utilizing the fake IP and MAC addresses provided in the message's ARP header. However, in practice, the success of this malicious activity depends both on the operating system deployed in the target host, and the existence of the IP and MAC addresses of the fake ARP entry in the target ARP cache before the attack attempt [3]. In fact, whether the malicious host uses fake ARP request or reply messages, there will be three possible cases that may occur. In the first case, the fake ARP message attempts to corrupt only the MAC address of an already existing ARP entry. In the second case, the fake ARP message attempts to corrupt only the IP address of an already-existing ARP entry. However, in the third case, the fake ARP message attempts to create a new fake ARP entry in the target ARP cache. That is, neither the IP address nor the MAC address of the fake ARP entry exists already in the target ARP cache.

VI. CONCLUSIONS

In the LAN environment security of information is not secure enough because of that hacker can easily perform MITM on the network. So this research work proving light weight approach for preventing the ARP poisoning in the network. In this research work is on Prevention of ARP poisoning on the network which is a part of MITM attack. Snort react in active way when its find malicious ARP packet in communication after that we propose scripting method for prevention and blocking that particular attacker. So attacker would not able to perform MITM again on the network.

VII. REFERENCES

[1]. S. Whalen, "An introduction to ARP spoofing," 2600: The Hacker Quarterly, vol. 18, no. 3, Fall 2001,.Available:http://servv89pn0aj.sn.sourcedns.com/_g bpprorg/ 2600/arp spoofing intro.pdf

[2]. D. Plummer. An Ethernet address resolution protocol, Nov.2010. RFC 826.

[3]. M. Carnut and J. Gondim. ARP spoofing detection on switched Ethernet networks: A feasibility study. In Proceedings of the 5th Simp´osio Seguranc¸a em Inform´atica,Nov.2010.

[4]. D. Bruschi, A. Ornaghi, and E. Rosti. S-ARP: A secure address resolution protocol. In Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC '03), Dec. 2011.

[5]. L. N. R. Group. Arpwatch, the Ethernet monitor program; for keeping track of ethernet/ip address pairings. (Last accessed April 17, 2012).

[6]. "ARP-Guard," (accessed 28-July-2013). Online. Available: http://www.arp-guard.com.

[7]. Snort Project, The. Snort: The open source network intrusion detection system. <http://www.snort.org>.

[8]. M. Tripunitara and P.Dutta. A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning. In Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99), Dec. 2013

[9]. N. Nikiforakis, Joosen, "HProxy: Clientside detection of SSL striping attack", Proceedings of the 7th Conference on Detections of Intrusions and Malware & Vulnerability Assessment, 2010.

[10]. A. Fung, K. Chueng, "SSLock: Sustaining the Trust on Entities brought by SSL, Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 2010.

[11]. M. Barnaba, "anticap", (accessed 17 April 2013) Online. Available: http://www.antifork.org/anticap.

[12]. V. Goyal and V. Abraham " An efficient Solution to the ARP cache poisoning problem", in Proceedings of 10th Australasian Conference on

Information Security and Privacy, Jul 2013, pp 40-51.
[13]. S. Y. Nam, D Kim and J Kim, "Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks" IEEE Common Lett, ol. 14, no. 2, (2010), pp. 187–189.
[14]. Arote Prerna, and Karam Veer Arya. "Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting."Computational Intelligence and Networks (CINE), 2015 International Conference on. IEEE, 2015.
[15]. Hou, Xiangning, Zhiping Jiang, and Xinli Tian. "The detection and prevention for ARP spoofing based on Snort."Computer application and System Modeling (ICCASM), 2010 International Conference on. Vol. 5. IEEE, 2010.
[16]. Akshada Hingne, Prof. Shitanshu Jain, A Survey on Various Detection and Prevention Mechanism for MITM and ARP Attacks, IJIRCCE.2016. 0411225
[17]. Avoiding Man in the Middle Attack Based on ARP Spoofing in the LAN, International Journal of Computer Applications Technology and Research Volume 5– Issue 5, 249 - 252, 2016, ISSN:- 2319–8656
[18]. Detection and Prevention against ARP Poisoning Attack Using Modified Icmp And Voting, Prerna Arote, Karam Veer Arya, 2015 International Conference on Computational Intelligence & Networks.
[19]. Detection and Prevention of ARP Poisoning in Dynamic IP Configuration, IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.