MAC POISONING ATTACK IN REAL TIME ENVIRONMENT

[1]Mohit Sharma, [2]Mamta Yadav
[1]MTech (CSE), [2]HOD of CSE DEPTT
[1]Computer Science of Engineering
[1]Yaduvanshi College of Engineering &Technology
Narnaul (Haryana)

Abstract: In today's world maintaining the security of information is a must. LAN is generally most common & very useful network in every organization. ARP is a mapping protocols from IP to MAC.ARP has two limitations. First it is a stateless protocol. And second no authentication process required for any host of the LAN. Attacker can easily exploit these vulnerabilities. There are many exiting solutions for ARP poisoning. Man-in-the-Middle (MITM) attack and denial of service (DOS) on ARP are very popular attacks. This paper presents all exiting solutions of MAC poisoning. It also represents some detection techniques and some prevention techniques. It also compares some scenarios with different mechanism for example SPOF, IP flooding, message flooding etc. In this paper, we would be analyzing the existing mechanisms and the works done by the researchers in early stages. Further we would be proposing a solution that would be contributing to the wealth of the domain.

Keywords: -ARP Spoofing/Poisoning, MIMA (Man in the Middle Attack), MAC Poisoning/Spoofing, Ettercap

INTRODUCTION:

ARP Stands for Address Resolution Protocol. It is used to convert IP address to physical addresses [MAC address] on a switch. The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address]. The resolved IP/MAC address is then used to communicate. It is also called as MIMA (Man in Middle Attack). Mac Poisoning is a method of exploiting the interaction of IP and Ethernet protocols. It is only applicable to Ethernet networks running IP. A computer connected to an IP/Ethernet LAN has two addresses. One is the address of the network card, called the MAC address. It is also called as Physical Address of computer and second in IP address each computer on a network must have a unique IP address to communicate. IP addresses are virtual and are assigned via software. IP and Ethernet must work together

MAC POISOINING

Address Resolution Protocol (ARP) is a protocol used for resolving IP addresses to machine MAC addresses. It is also called as MAC POISOINING or ARP Spoofing
Or MIMA (Man in the Middle Attack)

SPOOFING.

Working of ARP-

- When one system needs to communicate with another, it looks up its ARP table.
- If the MAC address is not found in the table, the **ARP request** is broadcasted over the network.
- All system on the network will compare this IP address to MAC address.
- If one of the system in the network identifies this address, then it will respond to the **ARP request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.
- **ARP POISOINING**

  ARP packets can be forged to send data to the attacker's Client System.
- ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.
- The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target system ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

LITERATURE SURVEY

M.G. and Huang,Gouda, C-T A Secure Address Resolution Protocol. Computer Networks, 41, 57-71 [2003] The authors assumed that there is a central server which maintains the database of the static entries of the MAC addresses of all the devices which lies on the LAN network. This approach does not work for the dynamic networks in which many nodes join and leave the network daily, where each node should be registered in the database before it can work. Also, the attacker can still generate the attack on the database. [4]

Issac, B. Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks. International Journal of Network Security, 8, 107-118 [2009] The authors proposed a unicast ARP request instead of the broadcast ARP request, with the help of a DHCP. In their approach, they assume that the DHCP will resolve the IP/MAC translation without the need for broadcast. However, the DHCP is at the application layer. Also, the DHCP may work only for dynamic IP addresses; it does not succeed for static IP addressing.[5]

Lootah, W., Enck, W. and McDaniel, P. TARP: Ticket-Based Address Resolution Protocol. Computer Networks, 51, 4322-4337 [2007] A Ticket-based Address Resolution Protocol (TARP) was proposed by Lootah, W., Enck, W. and McDaniel. TARP implements security by distributing centrally issued secure IP/MAC ticket with the help of the DHCP. These tickets are given to clients as they join the network and are subsequently distributed through existing ARP messages. These tickets include asymmetric digital signature, which has a considerable overhead in generating the public/private key pairs, and consumes more time. It is also not suitable for the dynamic networks where many new computers join the network frequently.[6]

Venkatramulu, S. and Guru Rao, C.V. Various Solutions for Address Resolution Protocol Spoofing Attacks International Journal of Scientific and Research Publications, 3, 2250-3153 [2013] The authors mentioned several resolutions and solutions to solve the ARP spoof problem and grouped them into cryptographic approaches, kernel-based patch, host-based approaches, port security on switch, manually configuration of static ARP entries, ARP spoof detection & protection software, server-based approaches and ASA (anti-ARP spoofing agent) software.[7]

Hong, S., Oh, M. and Lee, S. Design and Implementation of an Efficient Defense Mechanism against ARP Spoofing Attacks Using AES and RSA. Mathematical and Computer Modelling, 58, 254-260. [2013] the authors introduced a system that consists of a MAC-Agent and a Client-Agent. The MAC-Agent makes a reliable ARP table and sends the data to the Client-Agent, which prevents the host from using ARP. Instead, the Client-Agent receives the reliable ARP table information from the MAC-Agent and updates the ARP table information as static type. However, this solution requires cryptographic authentication techniques which are not 481 | P a g e

Available at the level of the data link layer. Additionally, this approach requires modifying the existing ARP protocol which is unpractical. [8]

Ramachandran, V. and Nandi, S. Detecting ARP Spoofing: An Active Technique. In: Jajodia, S. and Mazumdar, C., Eds., Information Systems Security, Springer, Berlin, Heidelberg, 239-250 [2005] The authors introduced a technique that includes collecting and analyzing the ARP packets, and then injecting ICMP echo request packets to probe for malicious host according to its response packets. However, this approach can be detected by the attacker and can be easily fooled. [9]

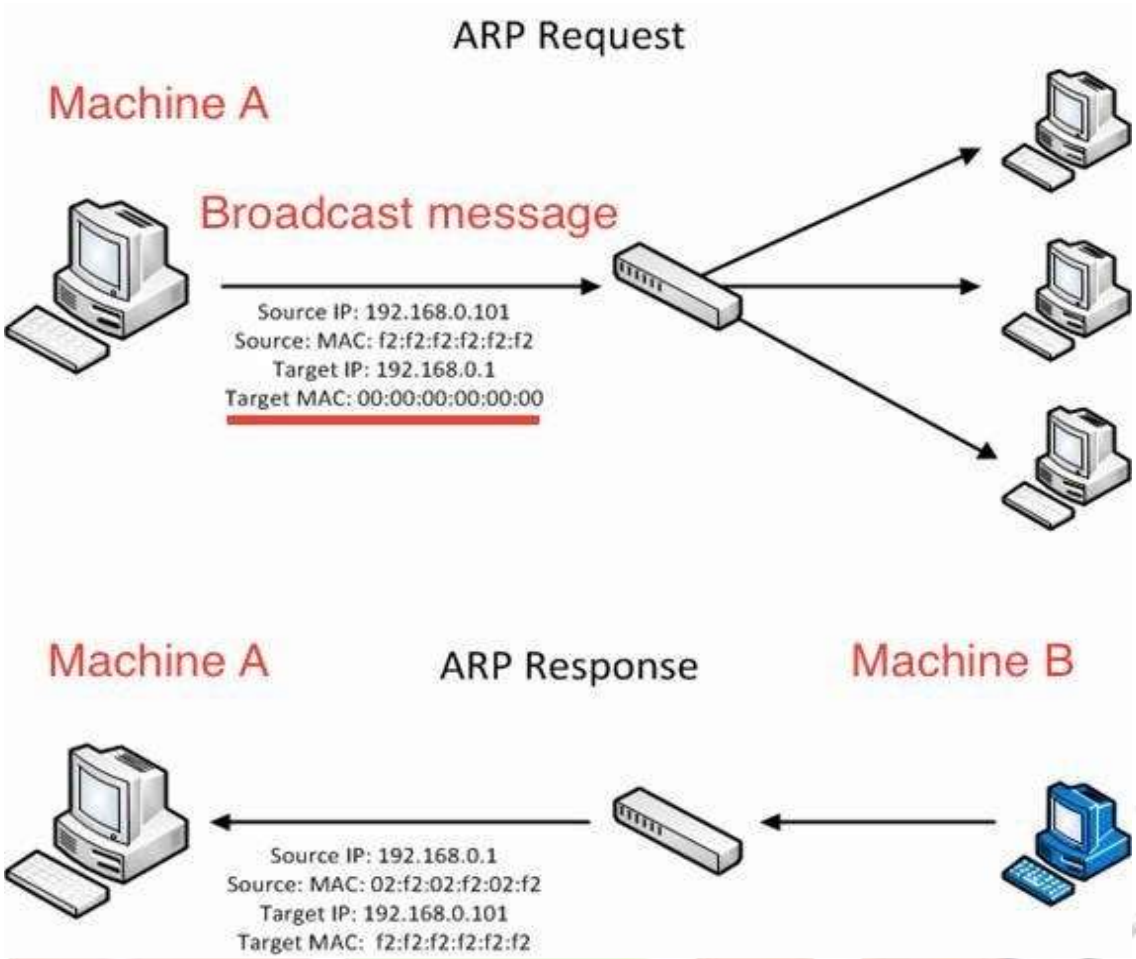
PROPOSED PROBLEM

As ARP updates the system's ARP cache table in the absence of reliable mutual agreement procedures while transmitting the request/reply messages, it has a few fundamental security problems. ARP spoofing attacks are described as follows.

i. Block host: an attacker, using the MAC Poisoning technique, can change the ARP cache table. The packets sent by the host, in which the ARP cache table is changed, do not reach the real destination address but reach the attacker. Thus, the host network can be blocked by the attacker.

ii. Host impersonation: an attacker can impersonate a host, and, by doing so, can discard the host's packet and cancel the host's request.

iii. Man-in-the-middle (MITM) attack: an attacker can change the ARP cache table of two hosts and monitor the communication between them.



Fig(1) ARP REQUEST

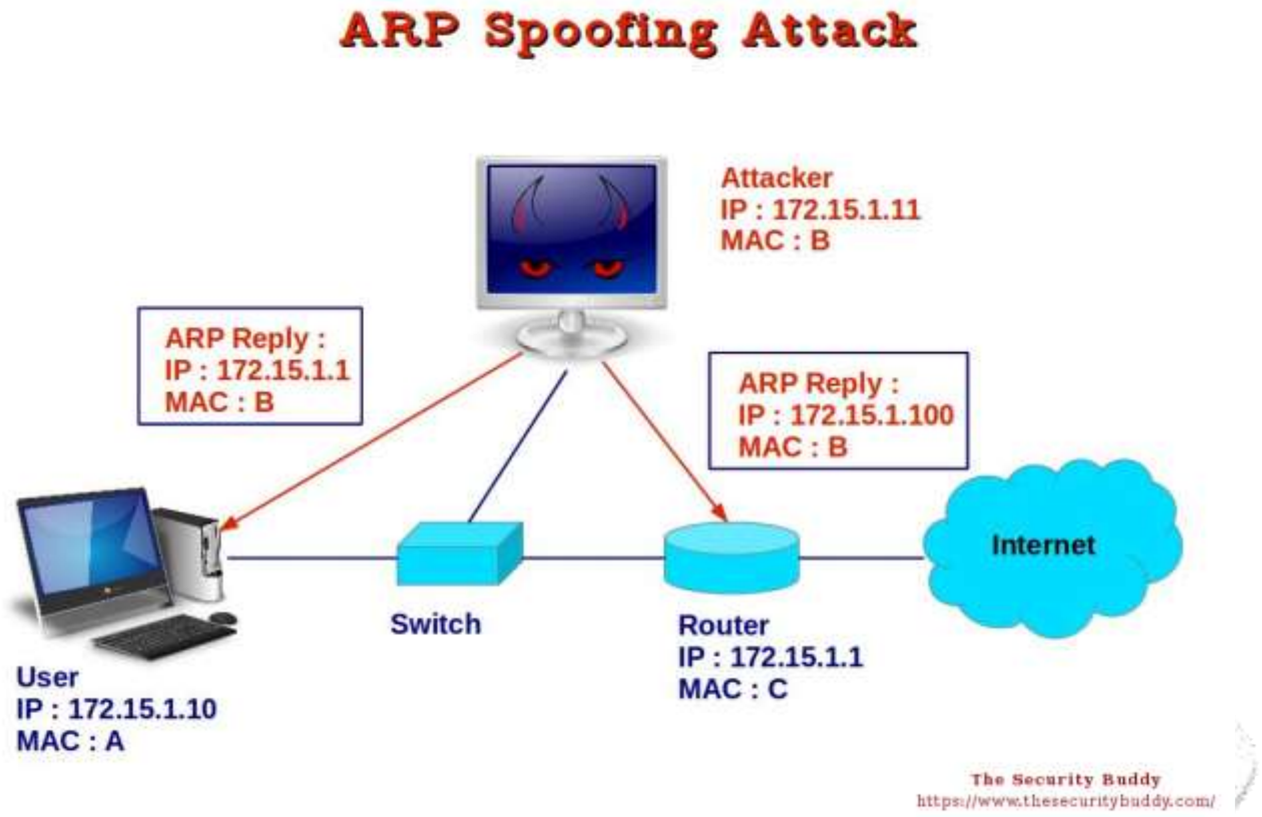


Fig (2) ARP SPOOFING ATTACK

In Figure 2, now the attacker mac address acts as a router mac address. The data from the user is sent via attacker device and then it passes through gateway.

DETECTION AND PREVENTION

Here are some of the methods that are employed in ARP spoofing detection and protection:

Authentication & Data Encoding

Authenticating a data sender's identity in some way can prevent receiving data from a malicious user. Authentication uses credentials from both the systems to authenticate the users. On top of that, the data is encrypted using some keys by the sender before sending it to the receiver. The encrypted data can only be decoded by some keys which have already been shared by the sender to the receiver beforehand. These things are a part of network security and especially encryption and decryption.

Packet filters

Packet filters are like inspectors which sit and carefully examine all the packets being transmitted across the network. Packet filters are often a part of the firewall programs which keep on looking out for the malicious packets.For example, a malicious packet could contain packets from outside the network that shows source addresses from inside the network and vice-versa.

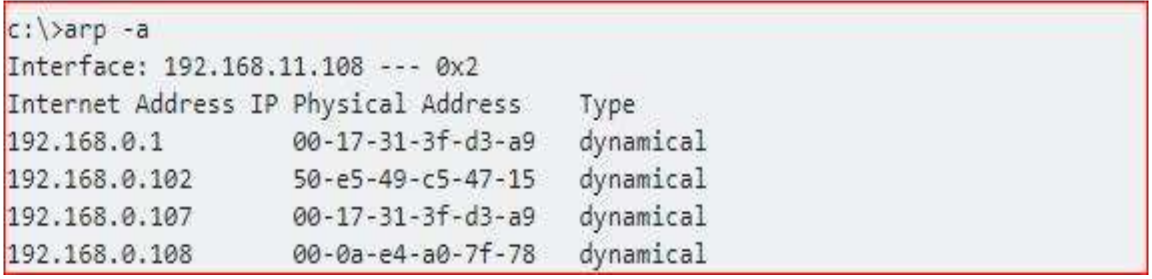
Using VPNs

Using VPNs (Virtual Private Networks) is one of the best ways to get protection against ARP spoofing attack (here are some best VPNs). A Virtual Private Network uses an encrypted tunnel for not only data transmission but also the data that goes through it is encrypted.

Use Anti-ARP Tools

Most of the methods mentioned above either require investment or are not completely failsafe such as Static ARP technique. It can only prevent simple ARP attacks. Some of the ways that Networks admins recommend are using anti-ARP tools to identify and stop the attacker.

This method is easy to implement and efficient to detect and prevent the ARP Spoofing attack



```
c:\>arp -a
Interface: 192.168.11.108 --- 0x2
Internet Address IP Physical Address   Type
192.168.0.1         00-17-31-3f-d3-a9   dynamical
192.168.0.102       50-e5-49-c5-47-15   dynamical
192.168.0.107       00-17-31-3f-d3-a9   dynamical
192.168.0.108       00-0a-e4-a0-7f-78   dynamical
```

Fig (3) Scanning IP

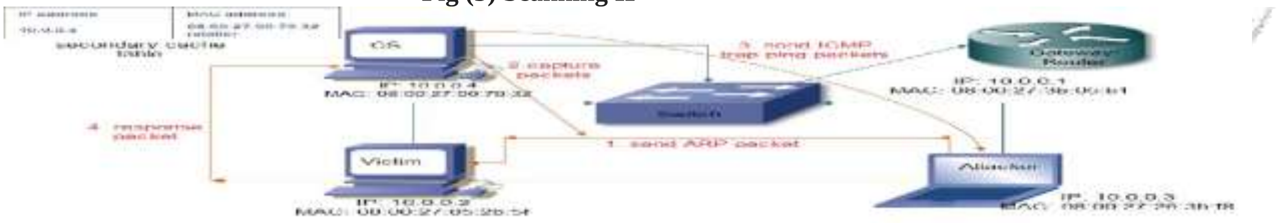
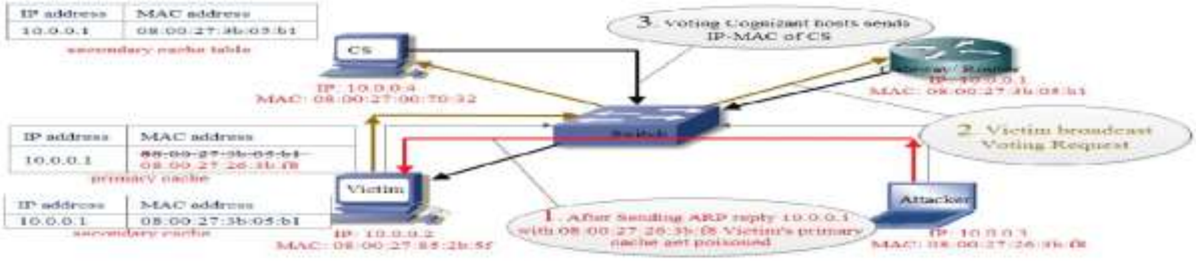


Fig. 2: Details of ARP Poisoning Detection



Fig(4)ARP SPOOFING DETECTION

CONCLUSION

This paper tried to explain ARP spoofing and proposed a solution to it and finally implementation was explained. There had been several proposals in the past as it is explained in section 3 of this document and as in [4]. All proposals have some advantages and disadvantages. But for the time being there is no widely available and known solution to this problem. Companies spend lots of money for firewalls and virus protection software. But they don't know how dangerous internal threats can be. A malicious worker can easily obtain passwords and the company confidential data through ARP spoofing. The AR server software like the one explained here will be very helpful to network administrators to defend their network against ARP spoofing.

REFERENCES

[1] D. Plummer. An ethernet address resolution protocol, Nov. 1982. RFC 826.

[2] W.Richard Stevens, TCP/IP Illustrated, Volume1. Addison Wesley, 2001.

[3] D.Bruschi, A.Ornaghi, E.Rosti, S-ARP: a Secure Address Resolution Protocol, Proceedings of the 19th Annual Computer Security Applications Conference, 2003

[4] Abad, Cristina L., Bonilla, Rafael I. An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks. Distributed Computing Systems Workshop, 2007. ICDCSW apos; 07. 27th International Conference on Volume, Issue, 22-29 June 2007 Page(s):60-60

[5] M. Gouda and C.-T. Huang. A secure address resolution protocol. Computer Networks, 41(1):57–71, Jan. 2003.

[6] V. Goyal, V. Kumar, and M. Singh. A new architecture for address resolution, 2005. Unpublished, available at .

[7] http://www.arp-guard.com

[8] ARP-GUARD, Welcome to the Future, White Paper, Version 2.0.1

[9] C. Schluting. Configure your Catalyst for a more secure layer 2, Jan. 2005. . (Last accessed April 17, 2006).

[10]Snort Project, The Snort: The open source network intrusion detection system, 2006.

[11]Incoming ARP packets can overwrite static entries in the ARP cache in Windows 2000, Microsoft Help and Support Article Id: 842168