Layer 2 Broadcast Attack: ARP Spoofing

CSC4209 Network Concepts and Practices

Ahmad Zulfahmi bin Harum
1626867

Haziq Iskandar bin Suriani
1628259

Hifdzul Hadi bin Daud
1620509

Abstract- **There are many attacks that can be happened in Layer 2 because Layer 2 is not designed for security and easy to be attacked. This paper will discuss Layer 2 broadcast attack specifically on Address Resolution Protocol (ARP) Spoofing. Layer 2 is Data Link layer according to Open System Interconnection (OSI Model) which provides node-to-node data transfer. Besides, this paper will enlighten few topics such as the problem description, prevention methods, solutions and so on.**

Keywords- **ARP, spoofing, data link, vulnerability, attack, OSI, model**

I. INTRODUCTION

Layer 2 acts as Data Link Layer in the seven-layer OSI reference model and equivalent to the lowest layer in the TCP/IP network model. The role of data link is to forward the smallest units of bits which is data link frame into devices on the same network. The common protocol that used at Layer 2 Ethernet protocol where it is implemented on the Network Interface Card (NIC) These days, most computers are connected to an Ethernet. Ethernet has two abilities which first is to memorize the MAC address of each port connected in order to forward to the appropriate address when the frame enters switch and second is the IP address.

In Ethernet protocol, the source need to be known in order to deliver stack for a packet to reach its destination; IP and MAC address. Using ARP can help the stack packets reach desired destination where it finds the MAC address destination computer by using the IP address destination. Even so, the security issues are being ignored in ARP design like all other TCP/IP protocol stack. For that, irresponsible people might be able to attack layer 2 using these protocols and ARP spoofing can be happened. ARP spoofing happens when the destination of request packets from other devices are being interrupted and force the destination to send the packets to attacker by tapping into communication. This situation is called *Man-in-the Middle* (MITM).

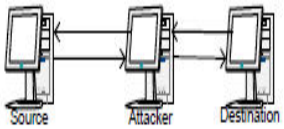

Figure 1.1 Man-in-the-Middle

When the attackers reach their goals in getting the packets, they may change content or inject new packets. This paper will focus more on ARP spoofing rather than the other attacks that are potential to be happened.

II. TYPE OF OTHER ATTACKS IN LAYER 2

Throughout years of technology, there are many attacks that already happened in Layer 2 beside ARP Spoofing. Below is the incomplete list of Layer 2 attacks;

1. Spanning Tree Protocol (STP) Attacks

STP is used on Local Area Network (LAN)-switched networks. If there are any potential loops within the network, removing them can be done by STP. Without STP, LANs in Layer 2 would stop functioning as the created loops within the network would flood the switches with traffic. Thus, if attacker inserts any new STP device on the network, the attacker has the potential to affect traffic flows through the LAN.

2. VLAN Hopping Attacks

This attack happens when a genuine VLAN connected to another VLAN is misled to hop or direct traffic by a switch. Two types of VLAN hopping attacks; switch spoofing and double tagging.

3. MAC Spoofing

The MAC address of an original and existing host is used where the attacker will spoofed ID rather than the original ID. Redirect all the traffic for the targeted device have been the purpose of the attack which to hijack phone number and having future calls rerouted to them.

4. CAM Table Overflows

The Content Addressable Memory (CAM) tables are used to track where to send traffic for specific learned MAC addresses. The attacker reaches the goals by floods the switch with fake packets containing fake MAC addresses.

These are the common attacks occurs in Layer 2 and probably there are attacks have not been discovered yet. Next section will enlighten more on ARP spoofing.

III. PROBLEM DESCRIPTION

ARP works between Layer 2 and Layer 3 of the OSI Model and it is used in TCP/IP network model at the internet layer. Address of a computer is determined by IP and MAC address at the Ethernet LANs using TCP/IP. Basically, the major role of ARP is to translate and map addresses; IP and MAC address. Internet Protocol (IP) commonly in use today for IPv4 is 32-bits long while MAC address is a psychical address with 48-bits long which MAC is interface address of NIC. A computer that joins a network (LAN) will be assigned a unique IP address. The purpose of the unique IP address is used for identification and communication. Besides, every NIC also has a unique MAC address.

Furthermore, when a computer has a packet to send, it will check the ARP cache first. ARP cache is the place where IP and MAC address mappings in pairs. The characteristic of ARP cache is that it has an aging time. When the aging time is at the end, the pairings are flushed from the cache. This is because of the dynamic nature of LANs. If there are no existing pairs of IP and MAC address, the new request is sent for network address and the ARP will start to perform and vice versa. For example, a source computer could not find the MAC address of the destination computer, it will broadcast an ARP request packet. Every host will check the IP address of the receive request whether it is in one of the network interfaces. If the IP address matches, it sends a unicast reply to the sender of the request with its pair address; IP and MAC address. Later, the pair will enter the ARP cache and start to perform for further use. When a host receives a reply, pair in the reply will updates the corresponding entry in the cache and a reply may be process even though request was never sent.

ARP Spoofing

ARP spoofing gives a great impact on enterprises. This attack can steal sensitive and confidential information even in it simplest form. ARP spoofing occurs by forging an ARP reply. The attacker may easily change the pair address (IP, MAC) that is contained in host ARP cache. To be clear, the attacker do a false ARP messages over the network (LAN) to get the MAC and IP address. The host will think that local cache to be trustworthy where it will send the encapsulated packets containing IP address with MAC address as destinations to the Ethernet frames.

Figure 3.1 Source of ARP cache and destination of host after attack

The attacker's goal is to associate the attacker's MAC address with the IP address of targeted host. In that case, any traffic meant for the host will be sent to the attacker's instead. In other words, the attacker will receive all the frames that are directed to the other host. Thus, both communication paths are under the attacker's control. Now the attackers could choose either to take a look at the packets, and then forward the traffic to the actual default gateway which later the data will be modified before forwarding it (man-in-the-middle attack) or the attacker could do a denial-of-service attack by dropping some or all of the packets on the LAN.

IV. DETECTION AND PREVENTION

There are several tools that can help to detect and prevent the ARP spoofing attack. All of the methods or tools have its own positive and negative impacts. The tools or method that could be used to detect and prevent ARP spoofing are:

1. Anticap

Anticap works with UNIX based operating system which is known by kernel patch. It is basically performs by rejecting ARP refreshes that contains MAC addresses that are not the same as the present table passage for that IP address.

This Anticap patch works in static conditions, yet it does not work in dynamic network (DHCP network) but it is accessible for a set number of working frameworks. The mechanism in this patch securing the ARP is where the heuristics blocking ARP replies at receiver. However, the

performance degradation was expected to be in a small number.

2. *Snort*

One of the famous Network Intrusion Detection System (NDIS) because it is lightweight yet very powerful. The features got in this tool are it has real-time, protocol investigation substance searching or match capacity. It can distinguish mixture of attacks and alarming the user in actual time. To make the snort stronger is by extending its plug-ins and adding ARP discovery module.in this way it can make the snort itself immuned and can work better as it can spot the attack more accurate in time.

3. *XArp 2 tool*

A tool that works by inspecting cross-layers of ARP. A host that runs the XArp 2 tool must connected to a SPAN port which is mirroring port which allow to receive and evaluate all the LAN network traffic. The system design is viewed as perfect as it is low cost and because of its effectiveness regarding the ability to detect ARP spoofing.

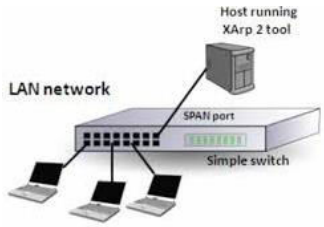

Figure 2. LAN network with XArp2 tool

It can be said that this is the most efficient security tool that able to handle ARP spoofing, anyhow it need some minimal improvement by creating an architecture that allow detection of ARP request storm and ARP scanning.

4. *Static entries in the ARP cache*

This is the most simple and somehow effective method to avoid ARP attacks. A new layer of protection can be formed by building static ARP entry which create a permanent entry in the ARP cache that helps to protect from spoofing.

However, there are two disadvantages which are it is inconvenient for the network administrator as it does not scale very well. The other disadvantage is that it cannot be performed in a dynamic environment, for instance a network with Dynamic Host Configuration Protocol (DHCP). In addition, it is only suitable for a smaller network and usually can prevent from simpler attacks.

V. SOLUTION

1. *ARP Spoof detection & protection software*

Some program has been built encounter ARP Spoof by detecting and protecting the devices effectively. Some of the portions are only built to detect and not to protect; XArp, ARPWathc. With this, user has to manually solute the attack or outsource another program.

2. *Cryptographic approaches*

Application of this method required asymmetric keys to verify the hosts in the local network area(LAN). This method is known as a secure address resolution protocol (SARP). First, each host will use invite-accept protocol to timely register its IP-MAC pairs in secure server. Then, the key pairs will be hashed by a message digest algorithm. This will require the sender to sign each ARP message with a private key and receiver will need to verify with the signature with the sender's public key. To authenticate a host, Goyal and Tripathy use a combination of digital signatures and a one time password based on hash chains. Another proposed methodology, ARP authentication scheme based on ARP authentication trailer (P-ARP), that uses magic number, nonce and HMAC hash function produce the authentication scheme based. It will hide the target IP address in ARP messages request. However, this technique is ineffective against ARP DoS attack.

3. *Layer-2 Switch Operation & Filtering.*

Using this approach, switch will be used for filtering based on the MAC Addresses and Protocol type of the Ethernet Frame. In a normal way, switch will look on the destination MAC address of incoming frame and look for it forwarding table. Switches will have the MAC and port number pairs in the table. Once it found the MAC address in the table then forwards the frame to the designated port. If not, it will forward the frame to all its port except the sender’s port. Furthermore, it also looks at the source of the address of the frame and if the pairs are not in the table it will update the table of it. In this technique, the switch will look extensionally at the source or destination MAC address and protocol type of the frame and apply the rules set by the admin to get rid of unwanted IP and ARP request.

4. *Ticket-based Address Resolution Protocol (TARP)*

This solution is introduced by Lootah that needs to implement security by distributing the centrally issued secure MAC/IP address mapping attestations through existing ARP messages.

5. *H. ASA (anti-ARP spoofing agent) software*

This type of solution requires an outsource software to intercepts unauthenticated exchange of ARP packets and block expected malicious communications. This suggested methodology does not require improvisation of kernel ARP software or installation of traffic monitors that will imply a costly upgrade to the hardware for both of the system. In spite of the fact that most has depend on computerized and energetic administration of ARP cache sections, current usage is well-known to be helpless to spoofing or denial of service(DoS) assaults. There are numerous devices that misuse vulnerabilities of ARP conventions, and past proposition to address the shortcomings of the 'original' ARP plan have been unsuitable. Recommendations that ARP convention definition be altered would cause genuine and unsatisfactory compatibility issues. Other proposition require customized equipment be introduced to screen noxious ARP activity, and numerous associations cannot bear such fetched. This consider illustrates that one can viably kill most dangers caused by the ARP vulnerabilities by introducing anti-ARP spoofing agent (ASA) which mediation unauthenticated trade of ARP bundles and pieces possibly unreliable communications.

6. Server-based Approach

Gouda and Huang proposed an engineering in which a secure server is associated with the Ethernet and communications with the server take control utilizing invite-accept and request-reply conventions. All ARP demands and answers happen between a host and the server, and answers are verified utilizing shared match keys. Kwon et al. proposed a comparative approach to safely oversee IP addresses in a distributed network. This approach employs an agent which recovers genuine IP–MAC sets from a host and advances them to the director to develop solid IP–MAC mapping. The supervisor hub monitors on the off chance that IP addresses of authorized hosts are changed, and unauthorized hosts are detached as they are expected to have endured spoofing assaults. Ortega et al. proposed a scheme that can be utilized to square ARP assaults in little office, domestic office (SOHO) LANs. The plot comprises of two components, specifically a server that upgrades the ARP cache and a switch that squares all ARP messages. Be that as it may, they fizzled to address.

Lootah et al. executed a secure IP–MAC address mapping in which an ARP answer is created with a connected signature when a ticket is issued. A ticket is added as a variable length payload. This approach deploys a local ticket agent (LTA), a key administration server, to issue public key to get the IP–MAC from the ticket. This approach is in reverse congruous with existing ARP, but it is vulnerable to replay assaults.

VI. CONCLUSION

In conclusion, we have research, study and analyse the topic of Layer 2 Broadcast attack specifically touch on the ARP Spoofing and we have acquired the prevention techniques of the attack and also solution to the problem that may lead to vulnerabilities. We analyzed several existing and available solutions and identifies the strengths and limitations of each solution.

VII. REFERENCES

[1] Abad, C. L., & Bonilla, R. I. (2007). An analysis on the schemes for detecting and preventing ARP cache poisoning attacks. *Proceedings - International Conference on Distributed Computing Systems*. https://doi.org/10.1109/ICDCSW.2007.19

[2] Al-Hemairy, M., Amin, S., & Trabelsi, Z. (2009). Towards more sophisticated ARP spoofing detection/prevention systems in LAN networks. *Proceedings of the 2009 International Conference on the Current Trends in Information Technology, CTIT 2009*, 225–230. https://doi.org/10.1109/CTIT.2009.5423112

[3] Hou, X., Jiang, Z., & Tian, X. (2010). The detection and prevention for ARP Spoofing based on Snort. *ICCASM 2010 - 2010 International Conference on Computer Application and System Modeling, Proceedings*, *5*(Iccasm), 137–139. https://doi.org/10.1109/ICCASM.2010.5619113

[4] Venkatramulu, S., & Rao, C. G. (2013). Various solutions for address resolution protocol spoofing attacks. International Journal of Scientific and Research Publications, 3(7), 1. https://pdfs.semanticscholar.org/7f6d/578bd50b25754189f63c37387e7422d4188a.pdf#page=678

[5] Arslan, Y. (2017). A solution for ARP spoofing: Layer-2 MAC and protocol filtering and arpserver. *arXiv preprint arXiv:1708.01302*.

[6] Cusack, B., & Lutui, R. (2015). Innovating additional Layer 2 security requirements for a protected stack.

[7] Elangovan, A. (2005). Efficient multicasting and broadcasting in layer 2 provider backbone networks. *IEEE Communications Magazine*, *43*(11), 166-170.

[8] Trabelsi, Z., & El-Hajj, W. (2010). On investigating ARP spoofing security solutions. *International Journal of Internet Protocol Technology*, *5*(1), 92.

[9] Goyal, V., & Tripathy, R. (2005, July). An efficient solution to the ARP cache poisoning problem. In *Australasian Conference on Information Security and Privacy* (pp. 40-51). Springer, Berlin, Heidelberg.