Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

ARP Spoof Detection and Mitigation

Mrs. Prema Arokiya Mary
Information technology
Kumaraguru College of technology,
Coimbatore, India

Mr. Sanjay M S
Information technology
Kumaraguru College of technology
Coimbatore, India

Mr. Vijayasenthil E
Information technology
Kumaraguru College of technology
Coimbatore, India

Mr. Abdur Rahman K
Information technology
Kumaraguru College of technology,
Coimbatore, India

Mr. Sabari B
Information technology
Kumaraguru College of technology
Coimbatore, India

Abstract: **Wireless Local Area Networks (WLANs) have become ubiquitous in modern connectivity landscapes, offering convenience and flexibility. However, they also introduce vulnerabilities, including Address Resolution Protocol (ARP) spoofing attacks, which exploit the inherent characteristics of WLANs to compromise network security. The proposed method begins by analyzing received ARP packets, extracting the source IP address to initiate a MAC address discovery process. An ARP broadcast is subsequently dispatched to retrieve the MAC address associated with the observed source IP. Notably, this approach leverages the inherent characteristics of ARP communication to efficiently correlate IP addresses with MAC addresses. The approach lies in the comparison between the MAC address from the received ARP packet and the newly discovered MAC address. If the two MAC addresses match, the ARP packet is deemed genuine; otherwise, it is identified as a potential spoofed packet. This innovative detection mechanism leverages the fundamental relationship between IP and MAC addresses, effectively distinguishing between legitimate and malicious ARP activities. To assess the effectiveness of the proposed approach, extensive experimentation is conducted within real-world wireless LAN scenarios, encompassing various network configurations and ARP spoofing attack scenarios. The results demonstrate a remarkable capability to accurately identify ARP spoofing attacks while minimizing false positives.**

Keywords **–** ARP spoof, MAC address, IP address wireless LAN.

I.INTRODUCTION

The Address Resolution Protocol (ARP) constitutes a pivotal protocol within both Ethernet and Wi-Fi networks, facilitating the mapping of IP addresses onto corresponding physical MAC addresses. Operating as a foundational aspect of local network communication, ARP's significance is equally pronounced in Wireless Local Area Networks (WLANs), albeit with adjustments tailored to the wireless environment.In the unique context of WLANs, ARP serves a parallel purpose to its wired network counterpart, albeit with an awareness of the wireless medium's intricacies. Here's a breakdown of how ARP functions within a Wireless LAN:When a device within a WLAN desires communication with another device, it necessitates knowledge of the recipient's MAC address, even though devices communicate primarily via IP addresses. ARP intervenes to bridge this divergence, effecting the resolution of a device's IP address to its corresponding MAC address.Consider a scenario where a device intends to dispatch data to a target peer but possesses solely the IP address of said peer. In this scenario, the initiating device initiates an ARP request packet, which is then broadcast across the local network. This broadcast assumes significance because the MAC address of the intended target remains unknown.Subsequently, a device possessing a matching IP address responds to this ARP request, generating and transmitting an ARP reply packet. This reply packet bears the device's MAC address, effectively enabling the requesting device to establish an ARP cache entry. This entry functions as a nexus between the IP address and the associated MAC address. As a result, subsequent communications with the same device are streamlined, guided by the ARP cache entry.Upon receipt of the ARP reply, the requesting device archives the IP-to-MAC mapping within its ARP cache. This cache assumes the role of negating the need for repetitive ARP requests targeting frequently accessed IP addresses. It's vital to note that the entries within the ARP cache possess a transitory nature and are susceptible to expiration as time progresses.

However, the Address Resolution Protocol (ARP) protocol notably lacks robust security measures that could effectively safeguard data integrity. This inherent vulnerability lays the groundwork for what is known as an ARP poisoning attack. In this form of attack, a malicious actor manipulates the MAC addresses within the ARP table, thereby opening the gateway for a Man-in-the-Middle (MITM) attack to occur. This research paper presents an innovative system designed to counter the threats posed by ARP poisoning attacks. The core principle of this system revolves around the meticulous analysis of incoming ARP packets. Upon receipt of an ARP packet, the system extracts the source IP address from it. Subsequently, a strategic maneuver takes place: the system disseminates an ARP request through broadcast.In the ensuing exchange, characterized by the ARP response or reply, the system successfully acquires the authentic MAC address of the original sender. A pivotal moment arises in the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

comparison between this garnered MAC address and the MAC address contained within the initially received ARP packet. Should these MAC addresses exhibit parity, the system categorizes the packet as bona fide and untampered. However, should disparities manifest between the two MAC addresses, a more ominous classification ensues: the packet is deemed malicious and indicative of a spoofing attempt.The efficacy of this system lies in its proactive detection of ARP spoofing incidents. Upon identifying a spoofed packet, the system promptly triggers an alert, thereby notifying relevant stakeholders of the breach. Moreover, the system goes a step further by providing explicit information regarding the attacker's IP address. This crucial detail serves as a starting point for potential mitigation strategies, potentially enabling the tracing of the malevolent actor back to their origin.In essence, this system contributes to the enhancement of network security by fortifying defenses against ARP poisoning attacks. By leveraging the strengths of ARP communication, it provides an additional layer of security to networks vulnerable to such exploits, thereby bolstering data integrity and thwarting the perilous Man-in-the-Middle attacks that ARP vulnerabilities can enable.

II. LITERATURE SURVEY

Paper [1] The first paper delves into the setup of IP forwarding on an attacker machine, enabling it to function as a gateway. The attacker then employs a tool called "arpspoof" to send deceitful ARP requests, thereby poisoning the ARP table. This manipulation can lead to potential security breaches and unauthorized network access.

Paper [2] In this paper, the author starts by offering a concise introduction to ARP and the concept of ARP poisoning. The focus then shifts to the categorization of detection techniques into three distinct classes: host-based, switch-based, and hybrid. Each technique is analyzed for its merits and demerits, providing a comprehensive overview of the different approaches to tackle ARP spoofing.

Paper [3] commences by detailing the operational dynamics of ARP and the vulnerabilities introduced by ARP spoofing attacks. Subsequently, it reviews existing solutions geared towards the detection and prevention of ARP attacks. These encompass diverse strategies, ranging from static ARP entries, cryptographic measures, and kernel patches, to network monitoring tools. The paper encapsulates a spectrum of potential countermeasures.

Paper [4] This paper introduces an inventive strategy for the identification and mitigation of ARP spoofing. This approach entails the establishment of a centralized server that maintains an exhaustive database housing IP-MAC mappings for all network hosts. By leveraging this repository, the server is empowered to discern legitimate communication from potentially malicious ARP activities, thus reinforcing network security.

Paper [5] In this paper, the author revisits the foundational concepts of ARP and ARP spoofing. Building upon this foundation, the paper proceeds to elucidate several existing methods devised to counter these security threats. Notable among these is the Dynamic ARP spoof protection and surveillance (DAPS) system, along with the ARP spoof detection software known as AVASS. These solutions exemplify real-world efforts to stymie the progress of ARP spoofing attacks.

Paper [6] This paper explores the utilization of machine learning algorithms for ARP spoofing detection. It delves into the development of a system that can discern anomalous ARP activities from genuine communications by learning patterns from network traffic data.

Paper [7] Focusing on enterprise environments, this research introduces a network segmentation approach to counter ARP spoofing. The paper presents the design and implementation of a system that compartmentalizes the network, reducing the potential impact of ARP spoofing attacks.

Paper [8] Addressing the limitations of existing ARP security mechanisms, this paper proposes a novel cryptographic protocol that ensures the integrity of ARP packets. By embedding digital signatures, it establishes a method for verifying the authenticity of ARP communication.

Paper [9] This paper explores the feasibility of hardware-based defenses against ARP spoofing. It introduces a specialized network device that intercepts and analyzes ARP traffic, effectively detecting and thwarting spoofed packets.

Paper [10] Focusing on real-time detection, this research presents an anomaly-based approach that employs statistical analysis to detect deviations from normal ARP behavior. The proposed system can promptly identify and respond to potential ARP spoofing incidents.

.

III. PROPOSED SYSTEM

The state-of-the-art ARP spoofing detection system harnesses the capabilities of the Scapy library within a Python framework, culminating in a user-friendly command-line interface (CLI) that streamlines interaction for optimal efficiency. This system represents a meticulously crafted response to the paramount challenge of identifying ARP spoofing attacks manifesting within a network environment.

The system's operational sequence is succinctly outlined as follows:

- Receipt of ARP Packets:

The system initiates by actively capturing incoming ARP packets circulating within the network. This foundational step forms the bedrock of subsequent analyses.

- ARP Broadcast for MAC Retrieval:

Building upon the collected ARP packets, the system orchestrates ARP broadcasts. The primary objective of these broadcasts is to elicit an ARP reply that furnishes the authentic MAC address associated with the source IP.

- Comparison of MAC Addresses:

A pivotal phase emerges as the system meticulously juxtaposes the MAC address garnered from the initial ARP packet with the MAC address gleaned from the subsequent ARP reply. This comparison serves as a litmus test, discerning the integrity of the received ARP packet.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

- Alert Triggering for ARP Poison Detection:

The system's efficacy in detecting ARP poisoning crystallizes at this juncture. If incongruity surfaces between the two MAC addresses under scrutiny, the system promptly triggers an alert. This alert serves as an immediate notification of a potential ARP poison intrusion. Concurrently, the system's display functionality comes into play, revealing essential information including the MAC address implicated in the spoofing attempt and the corresponding sender's IP address.

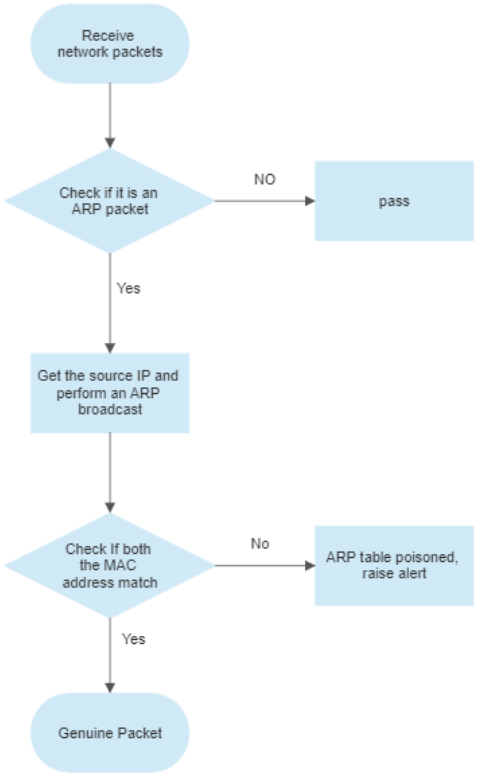

Fig 1. Workflow diagram

IV. WORKFLOW

Capturing Received ARP Packets:

Given the diverse array of packets coursing through network channels, the initial stride is to discern and isolate ARP packets from the broader traffic spectrum. Acknowledging that ARP doesn't monopolize network communication, the system begins by scrutinizing each incoming packet, filtering out non-ARP entities. Upon confirming an ARP packet's presence, the process advances to the subsequent stage of in-depth analysis.

Analyzing the Received ARP Packet:

The crux of this phase lies in the meticulous analysis of the ARP packet that has successfully met the criteria of being an ARP communication. To facilitate a comprehensive grasp, a comprehensive understanding of the ARP packet's structural composition is vital.

Before proceeding further, it's prudent to acquaint ourselves with the foundational blueprint of an ARP packet. This encapsulates essential components such as sender and target MAC addresses, IP addresses, and opcode.

By dissecting these components and delving into the ARP packet's intricate composition, the analysis phase endeavors to unveil critical insights. These insights could range from the identification of potential discrepancies in MAC and IP addresses to the dissection of opcode values, each of which contributes to forming a comprehensive picture of the packet's intent and authenticity.

In essence, this analytical stage serves as the vanguard of the system's operation. It empowers the system to effectively discriminate between genuine ARP communications and potential anomalies, ultimately contributing to the overall robustness of the ARP spoofing detection mechanism.

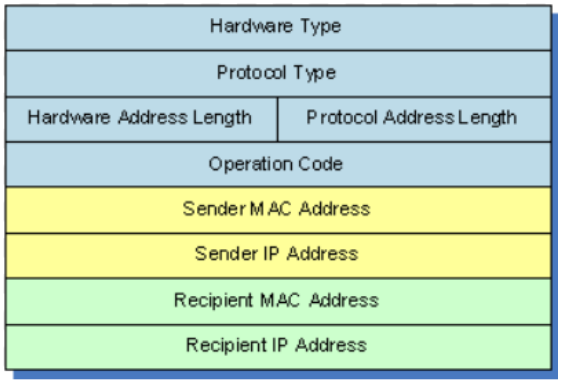

Fig 2. Structure of ARP packet

As visually depicted in Figure 2, the ARP packet encapsulates vital information encompassing both the sender's and receiver's IP and MAC addresses. This comprehensive set of data forms the cornerstone of ARP communication, facilitating the seamless mapping between IP and MAC addresses within a local network. Upon initial reception of an ARP packet, the system acknowledges that the authenticity of the sender's MAC address remains uncertain. To address this uncertainty, the proposed system initiates a strategic course of action. Starting with the sender's IP address gleaned from the received ARP packet, the system embarks on an ARP broadcast operation. This broadcast procedure assumes the form of a network-wide announcement, as the inquiring device transmits a message across the entire local network. This message poses a pivotal question: "Who possesses this particular IP address?" This inquiry reaches all devices within the network, effectively casting a wide net.

The magic happens when the device possessing the matching IP address responds to this broadcasted query. Armed with the corresponding MAC address, this responsive device relays its MAC address to the inquiring device. As a result, the inquiring device, now armed with the accurate MAC address, upgrades its ARP cache with this newfound information. The net effect of this meticulously orchestrated ARP broadcast sequence is the creation of a direct communication pathway at the data link layer. Subsequently, devices within the network can communicate

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

directly and optimally, circumventing the need for repeated ARP broadcasts to determine MAC addresses. This elevated efficiency in local network communication stands as a testament to the practical benefits of the ARP broadcast approach.

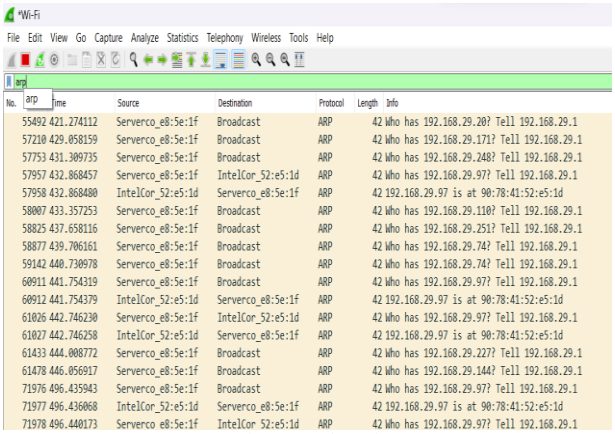

Fig 3 ARP broadcast

Figure 3 provides an illustrative representation of the ARP broadcast mechanism in action. This visualization enhances our understanding of the ARP broadcast process.Operating within this framework, the system deploys ARP broadcasts as a central strategy. When an ARP request is generated by the system, it traverses across the entire network, effectively reaching every connected device, inclusive of potential attackers.

In the case of the attacker, who possesses the requested IP address, a response is triggered. This response materializes as an ARP reply packet, encompassing crucial data: the original MAC address corresponding to the IP address in question. This MAC address is a cornerstone in the process of confirming the authenticity of the ARP packet. With the acquired original MAC address in hand, the system pivots to a pivotal point: a meticulous comparison against the MAC address initially extracted from the ARP packet. This comparison acts as the ultimate gauge of the ARP packet's credibility. Should the two MAC addresses align harmoniously, the system confidently classifies the packet as genuine. This congruence validates that the ARP communication is untampered, and network security remains intact. However, should disparities emerge between the two MAC addresses, a stark realization surfaces: the received packet bears indications of malicious intent. Specifically, this incongruity highlights the potential poisoning of the ARP table, signifying a potential breach.

Raise an alert:

Once it detects such malicious activity it immediately raises an alert, and also it displays the original and spoofed MAC address along with the IP address of the attacker machine.

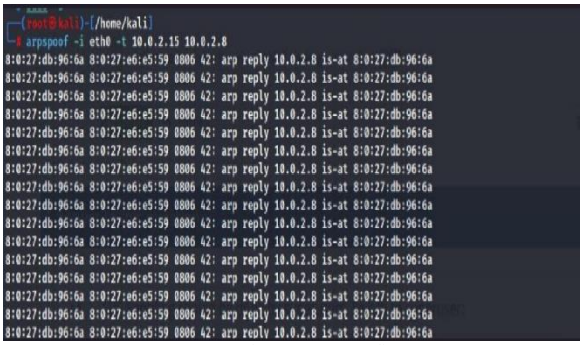

Fig 4 ARP spoofing

In Fig 4 the attacker is performing an ARP spoof attack on the victim,

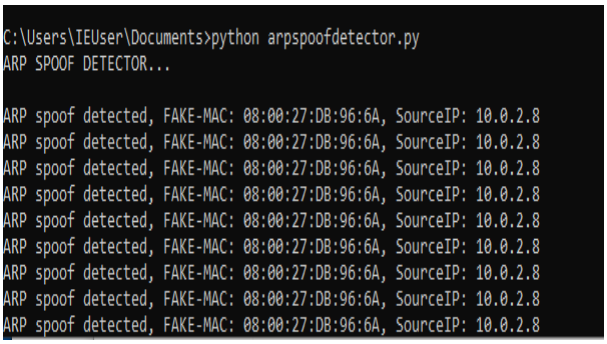

Fig 5 detecting ARP spoofing

In fig 5 in the victim machine the ARP spoof detector tool, actively analyses the received ARP packets to check for malicious packets, as mentioned earlier, it sends a ARP broadcast to find the real MAC address of the source IP from the ARP packet, and then checks whether both the MAC address matches, if it does , it is a safe packet, else it is malicious, then raises an alert displaying the fake MAC address and the source IP

V. MITIGATION TECHNIQUES

i) Static ARP tables**:** This involves mapping of MAC addresses to IP addresses. This can be done but it is heavy on the part of the administration. ARP tables keep a record of all the mappings and any network change is updated in these tables manually. Now, manually updating ARP tables for all hosts is not feasible for organizations.

ii) Switch Security: Most Ethernet switches have features that can help mitigate ARP Poisoning attacks. These features are also known as Dynamic ARP Inspection (DAI) and help in validating the ARP messages and drop packets that show any kind of malicious activity. This also allows one to limit the rate at which ARP messages can pass through the switch.

iii) Use Virtual Private Network (VPN). This will tunnel your traffic and protect your data from the attacker

CONCLUSION

In this paper we've studied the theory behind how the Address resolution protocol poisoning works and it's mitigation techniques, We've proposed a method to differentiate genuine packets with malicious ARP packet by sending ARP broadcast and using the MAC address received

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

to check for malicious packet, and also discovers and displays the original MAC address and the IP of the source device.

REFERENCES:

[1] Nagendran. K, Adithyan. A , Balaji. S , S.Balakrishnan1 "Sniffing HTTPS traffic in LAN by Address resolution protocol poisoning" https://acadpubl.eu/hub/2018-119-12/articles/7/1671.pdf

[2] Rajeev Kumar, Ankit Kumar, and Rakesh Kumar Detailed survey of ARP poison detection and mitigation techniques. https://www.researchgate.net/publication/313616135_A_Detailed_Survey_of_ARP_Poisoning_Detection_and_Mitigation_Techniques.

[3] S. Sivakumar, R. Sathishkumar, K. Sathishkumar, and M. Prabakaran "A Survey on ARP Spoofing and Prevention of ARP Attacks" https://www.ijrar.org/papers/IJRAR2001534.pdf

[4] Srinath Doss, Ramesh Babu Durai, Arun Prasath Gunasekaran, and Naveen Kumar Rajendran "Detection and Prevention of ARP Spoofing using Centralized Server" https://www.researchgate.net/publication/276932190_Detection_and_Prevention_of_ARP_spoofing_using_Centralized_Server

[5] Francis Jason, Amitha Joseph "A Review on ARP Spoofing Detection and Prevention "https://www.ijsr.net/conf/ICIPR2021/ICIPR2021_13.pdf

[6] ARP poisoning mitigation https://www.geeksforgeeks.org/how-to-avoid-arp-poisoning/

[7] Danish Javeed, Umar MohammedBadamasi, Cosmas Obiora Ndubuisi, Faiza Soomro and Muhammad Asif https://www.researchgate.net/publication/347006863_Man_in_the_Middle_Attacks_Analysis_Motivation_and_Prevention.

[8] Avijit Malik "Man in the middle attack understanding in simple words" https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/download/3453/2707

[9] Zouheir Trabelsi and Khaled Shuaib, Spoofed ARP Packets Detection in Switched LAN Networks. pp. 8191, 2008

[10] M. Gouda and C.-T. Huang, A secure address resolution protocol, Computer Networks, 41(1):5771, Jan 2003.

