ARP Poisoning (Address Resolution Protocol Poisoning)

Nithika T , Thivakaran S J , Eniyavan K
III B.Sc Digital Cyber & Forensic Science
Nehru Arts & Science College Coimabtore-641105
DR.WINSTON DUNN
Asst.Professor
Dep.of Digital Cyber &Forensic Science
Nehru Arts & Science College , Coimbatore-641105
nascasfar@nehrucolleges.com

I. ABSTRACT:

ARP (Address Resolution Protocol) poisoning, also known as ARP spoofing, is a network attack technique where an attacker sends false ARP messages within a local area network to associate their own MAC address with the IP address of another device, typically the gateway or another host. This manipulation enables the attacker to sniff, monitor, modify, or disrupt network traffic, ultimately leading to the loss of data privacy, MiTM-attack, or unavailability of service.

ARP poisoning is an attack that abuses the ARP protocol, which does not have security mechanisms to confirm the genuineness of the ARP messages. In this review, we are going to take a look at what exactly is ARP poisoning, and expose the various attack types that it is associated with, including the MITM and DoS attacks.

Furthermore, we will also investigate solutions to ARP poisoning and present methods for staged ARP scan, networks splitting, VPN, DHCP snooping, and NAC administrative control systems.

Ethical considerations and the legal implications of using ARP poisoning for malicious purposes are also examined. The paper concludes with recommendations for securing networks against ARP poisoning and enhancing overall network resilience against such attacks.

➢ **Key words** : ARP Poisoning, Address Resolution Protocol (ARP) ,Man-in-the-Middle (MITM) Attack , Denial of Service (DoS) Attack, Network Security

II. Introduction

ARP (Address Resolution Protocol) poisoning, which is also referred to as ARP spoofing, is a form of cyber attack that is usually perpetrated against local area networks. It is a method of the attacker who can walk in between another device and the router and intercept the traffic. In the first case, Alice's IP address is associated with Alice's MAC address, while Bob's IP address is associated with Bob's MAC address. In the third example, Alice's IP address is associated with Alice's MAC address, while Bob's IP address is associated with Bob's MAC address. An attacker plants malicious software in a network which breaks the end-to-end communication process between Alice's and Bob's devices. If Bob is a false IP, Alice's device sees the attacker MAC address as the one for Bob's, and the ARP table of Alice shows the MAC address of the attacker as being the one for Bob's IP address. The attacker's MAC address is used instead of the actual one so as to steal the data.

In this detailed explanation, we can analyze the topic of ARP poisoning - which is a method used by both attackers and defenders in digital security - and we can review how it works, its consequences, which are some of the measures that can be adopted to detect and prevent such attacks and what is the defense against such an attack.

How ARP Works (ARP Basics)

Before understanding ARP poisoning, it’s essential to understand the basic operation of ARP:

- ARP Request: When a device on a network wants to communicate with another device, it needs to know the recipient's MAC address. If the MAC address is not in the local ARP cache (a table that maps IP addresses to MAC addresses), it sends out a broadcast ARP request to the entire network, asking, "Who has this IP address?"
- ARP Reply: The device that owns the IP address responds with an ARP reply, which contains its MAC address. The requesting device stores this mapping in its ARP cache for future use.
- IP to MAC Mapping: This process allows devices to map the logical IP addresses to the physical MAC addresses on the local network, facilitating data transmission at the data link layer (Layer 2 of the OSI model).

What is ARP Poisoning?

ARP poisoning (or ARP spoofing) takes place when the malevolent entities send false ARP replies to the different devices pretending to be the part of the target chain and set a fake virtual connection with one of them by broadcasting fraudulent IP-destined ARP requests. Consequently, the various malicious ARP packets that incorporate the derivation of several intellectual property (IP) addresses such as the target's IP and the gateway IP address which have the attacker's Media Access Control (MAC) address which is claimed to be the rightful mapping, will enter the network. This will be noticed by the target devices on the network as they will update the ARP cache of their own, connecting the alleged attacker's MAC address to the IP address of the rest of the network devices.

Given the explanation mentioned before, the malefactor brings about the ARP cache of the devices being poisoned by setting their MAC addresses with the IP addresses of other devices. This process is the gateway for an offender to control the network traffic.

How APA Poisoning is Done?

Research of effects Connectivity on Computer Networks:

Step 1: The hacker, by means of some programs like Ettercap, Cain & Abel, or arpspoof, uses ARP packets that are uncharacteristically honest to pretend that they are the default gateway or the host (other than the target device).

Step 2: All the devices that are in the network, of which could be the victim's computer as well as others, are told of the false ARP reply by the attacker that replaces their ARP caches with the MAC address of the attacker.

Step 3: The victim's data now moves automatically to the hacker's computer. The attacker can be present in the interception of traffic and the equipment as it fights for the control of the attack as well.

- **Impact on Network Traffic:** The poisoned ARP tables cause the devices to send their data to the attacker's machine instead of the legitimate destination.
- **Interception:** The snooping of data like passwords, email, and personal messages is a method.
- **Change:** Change the information that is going between the devices, for an example, inserting a malevolent programming code or even changing financial transactions.

- **Drop**: Drown the attack by the packets being dumped or the devices not being able to communicate with each other.

III. Types of ARP Poisoning Attacks:

- **Man-in-the-Middle (MITM) Attacks:**

  This is the main reason for the peril in using ARP poisoning. The attacker places themselves in the middle of two communicating devices, thus making it impossible for the victim to understand that the data would be intercepted. The attacker can spoof the vendor's MAC address and submit it instead of the legal target address.

- **Denial of Service (DoS):**

  Improper behavior can cause the ARP cache to be improperly used, which will force the devices not to be able to communicate with each other. For example, a malicious actor can make a victim traffic transfer to an incorrect MAC address and thus disrupt the network.

- **Session Hijacking**:

  An attacker may listen to encrypted traffic and then hijack session cookies or gain unauthorized access by using application layer attacks. The hacker is able to make a user tick off receiving harmful code by sending packets to the target through this route.

- **Traffic Manipulation**:

The attacker has the power to modify the traffic that is sent to the primary source before forwarding it. This may include changing the names of the fraudulent accounts that harm their owners or the penetration of the destructive software with ill intent.

IV. Step by Step Example for ARP Spoofing:

1. **Step 1:** By means of an ARP spoofing utility, the attacker sends ARP packets to the host machine (Host A), thus falsely associating the MAC address of the real gateway device (Router) with the IP address of the host.

2. **Step 2:** The attacker uses the ARP packets also to notify the gateway (Router) that their MAC address is associated with the IP address of the Host A.
3. **Step 3:** At this moment, Host A misdirects its traffic, meant for the gateway, to the attacker's machine, believing it's the gateway. This eventually allows the attacker not only to forward the data on to the router, but also to decide whether or not the data can be changed in transit.
4. **Step 4:** In the same fashion when the router sends any data to Host A, the attacker can interfere with the data flow. In this way, the attacker is capable of either watching the flow of the data or interfering with it and making it different for the Host A and the router.

V. Consequences of ARP Poisoning:

1. **Data Theft:**

The hackers can easily access and steal the necessary details such as usernames, passwords, and bank details, thus making it easier for them to steal your identity or money by fraud.

2. **Traffic Manipulation:**

The hackers can intercept communications, therefore corrupt data, insert malware, etc., furthermore, redirect the communications to a malicious server too.

3. **Network Disruption:**

Varying the flow of the network traffic, or flooding the network with fake and malicious ARP packets, the attackers can considerably weaken or shut down the network service.

4. **Security Breaches:**

A breach in security that leads to attackers gaining access to protected networks can also potentially enable them to gain unauthorized entry into vital, private data, for example business files, intellectual property, as well as private communications.

5. **ARP Table Inspection**: One method to detect ARP poisoning is by examining the ARP table for unusual entries. If multiple IP addresses map to a single

VI. Detection of ARP Poisoning

1. Network Monitoring Tools:

Tools such as Wireshark, Cain & Abel, or Nessus can be used to capture network traffic and identify anomalies in ARP packets. For example, if ARP replies come from an unexpected source, it can indicate a spoofing attempt.

2. Intrusion Detection Systems (IDS):

IDS systems can help monitor network traffic and detect suspicious ARP activity, alerting network administrators about potential ARP poisoning attacks.

VII. Prevention of ARP Poisoning:

- **Static ARP Entries**:

  Setting static ARP entries on the main devices (e.g., the file server, the default gateway) allows you to avert the ARP cache from being updated dynamically and, thus, impersonation is also not probable. Nevertheless, this is unfeasible for large networks.

- **Network Segmentation**:

  Deployment of the most sensitive devices and systems in the different VLANs (Virtual LANs), will make the impact of attacks restricted. By disconnecting the workstations from the critical servers and routers, ARP spoofing can be confined and counteracted easily.

- **Encryption:**

  The usage of encrypted transmission methods such as HTTPS, SSH, TLS, and VPNs is the best way to make traffic unreadable or unalterable for an eavesdropper in the case of being caught. This is particularly crucial for pages, emails, and other data that are confidential and are being used over the internet.

- **Dynamic ARP Inspection (DAI):**

  DAI is usually detected in most switches that have their setting managed. This feature checks that only approved means of sending ARP replies are used by ARP packet validation based on DHCP probing tables. DAI is capable of blocking unwanted ARP packets inserted into the network by hostile attackers.

- **Port Security**:

Port security on managed switches is done by setting up the maximum number of allowed MAC addresses on the port, this prevents attacks from flooding the network with faked ARP packets.

- **ARP Spoofing Detection Tools**:

Explore XArp extending ARP spoofing detection functionality or deploying Arpwatch (tools that analyze network traffic patterns). These programs are useful for monitoring the network for its security.

- **Ethical Considerations**

Although ARP poisoning is a reliable attack technique, it can also be transformed into an ethical one in the field of network security testing, which is also called penetration testing. Ethical hackers may use ARP poisoning in a controlled environment, to assess the security of the network and guide organizations in the reinforcement of their defenses. Yet, unauthorized use of ARP poisoning is illegal and a violation of privacy and data protection laws.

VIII. Conclusion

ARP poisoning is a remarkable tool for a hacker to attack the MITM on a local network. An ARP Update (ARP) is a critical aspect of two different attacks, such as MITM. The antics often prevail as a result of "faking" the numbers leading to depth. But also, the string calculation is another technique that fraudsters may use to manipulate addresses. Uninformed people or people who do not know how hackers can fake MAC addresses are likely to be victims of ARP spoofing. With the right detection tools, prevention strategies, and awareness, organizations can protect themselves from these attacks. The implementation of data scrambling, network monitoring, and preventive measures are some of the ways of effectively stopping ARP that is then aimed at stealing data, causing network interruption, or any other malicious activities.

IX. References:

B. Schneier, "Network Security: Private Communication in a Public World," Prentice Hall, 2019.

J. Beale, "Nessus: The Comprehensive Guide to Network Security Scanning," 2018.

S. McCumber, "Network Security and Cryptography," Wiley, 2021.