IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, February 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202051 |

A Survey on ARP Poisoning

Suma B, Murugan R

Student of MCA, Dept. of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India

Professor, Dept. of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India

ABSTRACT: This paper's primary goal is to examine the detection and mechanism of ARP spoofing. One may argue that the Address Resolution Protocol, or ARP for simple terms, is crucial to computer science and forensics. ARP spoofing is one of the various computers hacking techniques used nowadays by individuals to transmit phony ARP packets across a Local Area Network (LAN). Such attacks might lead to changes in traffic patterns or, worse yet, a temporary or permanent stoppage of traffic. Even though this attack is only possible on networks with Address Resolution Protocols, ARP spoofing can be a precursor to more dangerous assaults that have the potential to do considerably more harm. An attacker seeking to launch this sort of attack will search for the Address Resolution Protocol's vulnerabilities. He may, for instance, be trying to take advantage of flaws like the message's inability to properly verify the sender. Because of this, hackers may find it very simple to alter or steal users' data. Because ARP spoofing poses a genuine risk to the security of every user on the network, all appropriate precautions must be taken to minimize harm.

KEYWORDS: ARP, ARP Poisoning, Attack Types, Detection, Inspection Tools, Manual Detection, Avoiding Methods, Comparison of ARP Poisoning Countermeasures.

I.INTRODUCTION

The Address Resolution Protocol (ARP) lacks a trustworthy means of confirming the sender's identity, it is well recognized to be very vulnerable to spoofing attacks. Sometimes the absence of state makes an attack more likely to be harmful. Attacks such as man-in-the-middle, denial of service, and session hijacking are examples of malicious activities that have the potential to seriously impair local area networks. The current methods are thought to be ineffective because they are passive in their detection of spoofing assaults. Monitoring the ARP traffic and looking for anomalies in the Ethernet takes time, which makes it difficult to identify the assault early on. This paper's primary goals are to describe an active methodology that detects ARP spoofing successfully and to illustrate a very helpful technique that forensic investigators may employ to obtain evidence straight from the source machine. The network security practice includes a talk on identifying ARP poisoning attacks.

II. BACKGROUND

A. ARP

The Address Resolution Protocol (ARP) is a protocol that uses the IP address to determine the physical address (MAC address) of a matching host. Its full name is "Address Resolution Protocol".

The ARP protocol is part of the TCP/IP protocol, which is situated at the network layer of the TCP/IP five-layer architecture. Its function is to resolve an IP address into a MAC address. In a local area network, this protocol is used to resolve the physical address that corresponds to the IP address.

To explain, an IP datagram sent by host A to host B over the network is received by the router on the network where host A is located first. The router then checks to see if the destination address is part of the network and, if it is, forwards the datagram directly to the destination host in this network; if not, it passes on to the next route until it reaches the router of the specified network, which then forwards the datagram to the destination host.

At some point, the entire procedure will entail a network router (or gateway) transmitting data to a host on the network. Since the data transmission of the data link layer is transmitted through the physical address, the router typically initiates this process by sending an ARP broadcast request, asking the host whose IP address matches the destination IP address of the data packet to return its own MAC address to the router.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202051 |

Every host on the LAN will receive the broadcast of the ARP request. Check the IP address of the host that submitted the

ARP request, save it in the ARP cache together with its accompanying MAC address, then check this when additional

hosts on the network receive the ARP request. It sends an ARP reply with its own IP address and accompanying MAC address, regardless of whether the IP address sought in the ARP request is its own IP address. The network router can successfully send the data packet to the destination host via the data link layer after it has obtained the MAC address.Before

delivering the frame, the host performs a procedure known as "address resolution" in which it changes the target MAC address from the target IP address. In order to guarantee seamless host-to-host communication, the primary purpose of the ARP protocol is to query the target device's MA address using the target device's IP address.

ARP and DNS share some similarities. The distinction is that DNS resolves domain names and IP addresses. Furthermore, ARP protocol does not require service configuration, but DNS does. Both communicating hosts have to be in the same physical network segment a local area network environment according to the ARP protocol.

B. ARP POISONING

ARP Poisoning is the practice of manipulating the MAC-to-IP mappings of other networked devices by taking advantage of ARP's vulnerabilities. When ARP was first launched in 1982, security was not a top priority, therefore authentication procedures for validating ARP messages were never incorporated in the protocol's architecture. Regardless of whether the original message was meant for it or not, any device connected to the network can respond to an ARP request. An attacker at Computer C, for instance, may answer to Computer A's "ask" for Computer B's MAC address and Computer A would regard this response as genuine. Numerous assaults are now conceivable as a result of this carelessness. A threat actor can "poison" other hosts' ARP caches on a local network by using readily accessible tools to add erroneous entries to the ARP cache.

III.AIMS AND OBJECTIVES

Attacking a machine on a secure network environment to trace weakness of the network by passive ARP poisoning and figure out probable route to makeover. Technically speaking, the attack will include poisoning the Address Resolution protocol to see what type of information about the target computer may be discovered while the target computer is persuaded to transmit reply packets through the attacker system. Because ARP is a stateless protocol, whenever a new ARP reply is received, the computer updates its ARP cache with the most recent one. This thesis thus focuses on how this may drive further research and how, in the end, we could respond to it.

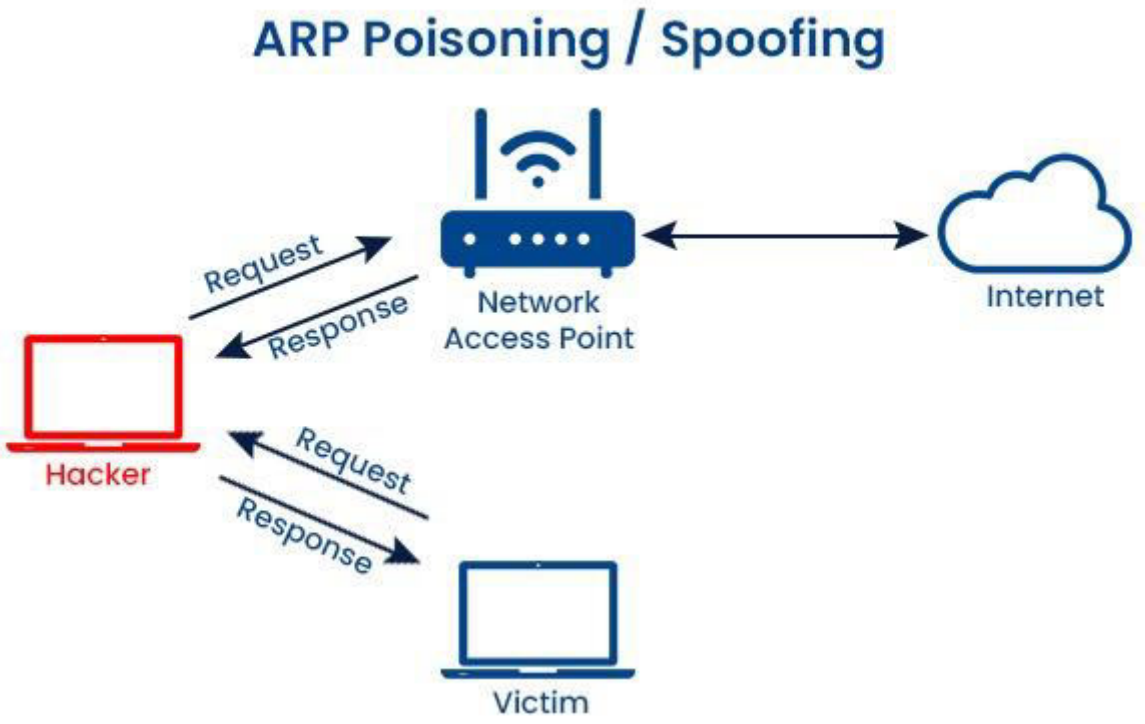
IV. WHAT IS THE MECHANISM OF AN ARP POISONING ATTACK?

In order to determine the IP and MAC addresses of the two devices that are in communication with one another, the attacker first watches the network traffic. These gadgets may include a router and the user's PC.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202051 |



- The user's PC then receives an unwanted ARP reply packet from the attacker. Its goal is to give its own MAC address and assert that it is the router's IP address holder.
- The user's computer then starts transmitting data packets to the attacker's MAC address rather than the router's MAC address by updating the ARP cache with fake information.
- Additionally, the attacker sends the router an unsolicited ARP reply packet. This asserts once again to possess the user's computer's IP address before supplying its own MAC address.
- Additionally, the router begins forwarding packets to the attacker's MAC address rather than the user's MAC address by updating its ARPO cache with the bogus mapping.
- After completing the aforementioned actions, the attacker is ready to insert itself into the middle of the conversation between the user's computer and the router. Data packets passing through it can now be readily intercepted, altered, or dropped by the attacker.

V.DIFFERENT ARP POISONING ATTACK TYPES

After gaining access to the system through ARP poisoning, attackers are able to move around and intercept any communications that are sent between the program and the network. Once access is obtained, attackers have the ability to conduct more dangerous application assaults, such as:

Man-in-the-middle (mitm) attack

The most frequent and maybe riskiest objective of ARP poisoning is certainly MiTM assaults. An IP address, usually the default gateway for a certain subnet, is sent out by the attacker via fake ARP answers. Because of this, the attacker's machine's MAC address appears in the ARP cache of the victim computers rather than the MAC address of the local router. Network traffic will subsequently be mistakenly sent to the attacker by victim workstations. By acting as a proxy and seeing or altering data before transferring the traffic to its intended location, the attacker can be enabled by tools such as Ettercap. All of this could seem natural to the sufferer.

The efficacy of a MiTM attack can be significantly increased by combining DNS poisoning with ARP poisoning. In this case, the victim user may enter in the IP address of the attacker's machine instead of the real address on a website like google.com.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202051 |

Distributed denial-of-service (ddos) attacks

The goal of a denial-of-service (DoS) attack is to prevent one or more victims from using network resources. An attacker might theoretically overwhelm the target system by sending out ARP Response signals that erroneously map hundreds or thousands of IP addresses to a single MAC address. ARP flooding, another name for this kind of attack, can also be used to target switches, which could have an effect on the network's overall performance.

Session hijacking

Man-in-the-Middle attacks and session hijacking attacks are similar in that the attacker does not send communication from the victim system straight to the intended destination. Rather, by obtaining a legitimate TCP sequence number or web cookie from the victim, the attacker will be able to take the victim's identity. Should the target person be signed in, this might be exploited, for example, to get access to their social network account.

VI. DETECTING ARP POISONING

Identification of ARP poisoning is the first line of defense against assaults. Keep an eye out for the following signs and symptoms that might point to ARP poisoning:

Network slowdown

ARP poisoning may be the cause of a notable drop in network performance and data transmission speed. Keep an eye out for any unexpected or inexplicable slowdown in your network.

Unusual or unexpected network behavior

ARP poisoning may be the cause of unusual or unexpected network behavior, such as frequent disconnections, network outages, or the inability to access particular services.

Increased network traffic

An ARP poisoning attack may be detected by an abrupt spike in network traffic or a noticeable rise in the quantity of ARP requests and answers.

VII.TOOLS FOR ARP INSPECTION

ARP poisoning attacks may be found using a variety of methods. These tools are useful for keeping an eye on network traffic, deciphering ARP signals, and warning users of any questionable activity.

ARPWatch

When irregularities or unauthorized changes arise, ARPWatch notifies network managers by keeping an eye on the ARP cache and identifying modifications in IP-to-MAC address mappings.

Wireshark

An efficient tool for assessing communities is Wireshark, which records and examines network traffic made out of ARP packets. Examining ARP messages, administrators can identify anomalous or malevolent ARP activity.

Tools for network monitoring

Robust network monitoring programs, like Nagios or PRTG Network Monitor, can analyse traffic patterns, watch network behavior, and sound an alert when they detect questionable ARP-related activity.

Arp-guard

Pull up a visual representation of your current network, complete with switches and routers. Permit the software to learn what devices are connected to your network so that it may create rules to manage connections going forward.

XARP

To find assaults taking place behind your firewall, use XArp. Receive alerts as soon as an assault starts, and utilize the tool to decide what action to do next.

VIII. METHODS OF MANUAL DETECTION

To find possible ARP poisoning attacks, manual detection techniques can be used in addition to specialist instruments.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202051 |

Among these techniques are:

Examining ARP cache
Discrepancies or questionable IP-to-MAC address mappings can be found by routinely checking the ARP cache on networked devices.

Analyzing network logs
One useful way to monitor network activity is to go through and analyze network logs. Any unusual or questionable ARP queries or messages from any device fall under this category.
Network administrators may greatly improve their ability to quickly identify ARP poisoning attacks by combining automated ARP inspection tools with manual detection strategies.

IX.HOW TO AVOID POISONING FROM ARP

The key to preventing ARP poisoning on your network is to successfully lower the likelihood of such attacks by putting in place basic preventive measures. A few simple yet powerful preventative techniques are as follows:

1. Network infrastructure that is secure
To provide a secure network infrastructure, adhere to recommended procedures like:

Strong passwords: To reduce the danger of unauthorized access, enforce the use of strong and distinctive passwords for all network devices, including servers, routers, and switches.

Frequent firmware updates: Make sure network devices are running the most recent firmware versions available from the makers. Security patches and bug fixes that address vulnerabilities are frequently included in firmware upgrades.

Disable superfluous services: In order to lower the attack surface and restrict possible points of entry for attackers, disable any superfluous network services or features that are not in use.

2. Segmenting networks
Implement network segmentation to separate your network into logical subnetworks. ARP poisoning attack effect is reduced by dividing devices into smaller, more isolated networks. Other parts stay safe even in the event that one is breached.

3. Putting secure ARP configurations in place
Set up secure ARP settings (Static ARP Table Entries) on your network devices: Set up static ARP table entries by hand for your network's important devices. This guarantees that certain IP addresses are linked to only authorized MAC addresses.

- **Set up secure ARP settings (static ARP table entries) on your network devices**
  Set up static ARP table entries by hand for your network's important devices. This guarantees that certain IP addresses are linked to only authorized MAC addresses.

- **Systems for detecting and mitigating ARP spoofing**
  Certain network devices come equipped with built-in systems for detecting and mitigating ARP poisoning assaults. Turn these features on whenever you can.

- **Dynamic ARP inspection (DAI)**
  Some network switches have a security function called dynamic ARP inspection (DAI) that verifies ARP packets and looks for consistency in IP-to-MAC address mappings. Use DAI to stop ARP spoofing and confirm the legitimacy of ARP messages.

4. Intrusion detection and prevention systems
Install intrusion detection and prevention systems (IDS/IPS) equipped with modules made expressly to recognize and stop ARP poisoning techniques. These are going to keep an eye on network traffic and detect any unusual ARP activity.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202051 |

X. COMPARISON OF THE SEVERAL ARP POISONING COUNTERMEASURES

countermeasure	Type	Effectiveness	Complexity	Performance impact	Cost
Dynamic ARP Inspection (DAI)	Prevention	High	Moderate	Medium	Moderate
Port Security	Prevention	High	Moderate	Low	Moderate
Static ARP Entries	Prevention	High	High	Low	Low
Network Segmentation	Prevention	High	High	Variable	Moderate
Encryption (HTTPS, VPNs)	Prevention (Data Protection)	Medium	Low	Variable	Low
Network Monitoring Tools	Detection	High	Moderate	Variable	Moderate
Intrusion Detection Systems (IDS)	Detection	High	High	Medium	Moderate
ARP Spoofing Detection Tools	Detection	High	Moderate	Low	Moderate
Regular ARP Cache Flushes	Detection	Medium	Low	Low	Low

XI.CONCLUSION

ARP poisoning, which uses flaws in the Address Resolution Protocol to intercept and alter data flow inside a local area network, is a serious threat to network security. This malevolent method has the potential to cause eavesdropping, data modification, and unauthorized access, among other security lapses.

Establishing strong security protocols is essential for enterprises to reduce the hazards related to ARP poisoning. Network segmentation, encryption protocols, and ARP spoofing detection technologies may be used in this process. Regular network monitoring and user security awareness training can also help identify and stop ARP poisoning attacks early on.

The tactics used by cybercriminals evolve with technology. Thus, keeping up with the most recent advancements in network security and routinely upgrading security protocols are crucial elements of an all-encompassing defensive plan against ARP poisoning and other new threats. Organizations may better protect their sensitive data and preserve the integrity of their communication infrastructure by taking a proactive approach to network security.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202051 |

REFERENCES

1. Vivek Ramachandran, S. N. (2006). Detecting ARP Spoofing: An Active Technique. Retrieved March 5, 2012, from vivekramachandran.com: http://www.vivekramachandran.com/docs/arp-spoofing.pdf
2. M. Tripunitara and P. Dutta, "A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning", 15th Annual Computer Security Applications Conf., 1999, pp. 303-309.
3. B. Zdrnja, "Malicious JavaScript Insertion through ARP Poisoning Attacks", IEEE Security & Privacy, May/June 2009, pp. 72-74.
4. M. Kolodziejczyk and M.R. Ogiela, "Security Mechanisms in Network Protocols", 2010 Intl. Conf. on Intelligent Systems, Modeling and Simulation, 2010, pp. 427-430.
5. C.L. Abad and R.I. Bonilla, "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks", 27th Intl. Conf. on Distributed Computing Systems Workshops (ICDCSW'07), 2007, p. 60.
6. W. Lootah, W. Enck and P. McDaniel, "TARP: Ticket-based address resolution protocol", 21st Annual Computer Security Applications Conf. (ACSAC 2005), 2005, 9 pp. – 116.
7. D. Bruschi, A. Ornaghi and E. Rosti, "S-ARP: a Secure Address Resolution Protocol", 19th Annual Computer Security Applications Conf. (ACSAC 2003), 2003, pp. 66-74.
8. H. Salim, Z. Li, H. Tu and Z. Guo, "Preventing ARP Spoofing Attacks through Gratuitous Decision Packet", 11th Intl. Symp. on Distributed Computing and Applications to Business, Engineering & Science, pp. 295-300.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details