BUCKET BRIGADE ATTACK USING ARP SPOOFING

Harshit Rastogi, Dr. Krishnaraj N, Aravinth M.

Abstract— DNS spoofing is a method for altering DNS requests made by clients such that the IP address returned in the query is whatever the attacker desires. A Man-in-the-Middle attack should also be conducted for the DNS spoofing attack to be successful, and this can be done through ARP spoofing. A cyber related attack which is known as a "man-in-the-middle" (MITM) assault demands the perpetrator secretly interrupt and relay communication between two parties who trust they are talking with one another directly. The action of poisoning Domain Name Service - DNS server entries to lead a targeted user to a malicious website under the charge of the attacker is called DNS cache poisoning. This paper basically focuses on understanding the previous papers to understand about the attack that can be done through various techniques. By doing this research we will be able to do a depth analysis of DNS spoofing attack along with the Man-in-the-Middle Attack. Further this paper continues with the expected outcome along with the conclusion that is required for the attacks.

Index Terms— Cyber Security, Hacking, Network, Penetration Testing, Domain Name System Spoofing, Man-in-the-Middle Attack, MiTM Attack, Cyber Attack, ARP Spoofing.

1 Introduction

The amount of time people spend online is growing significantly over time. A rapid escalation of stock market value emerged in the late 1990s, a time of rapid expansion in Internet usage and consumption, from the internet bubble, also known as the dot-com boom, the technology boom, or the internet boom. The world of today is a digital one. The world is online. Almost every characteristic of our life is associated with the utilization of the Internet and cellular networks. All the internet services save and transfer user’s valuable data and details through some communication channels. [1] Hackers target the sensitive data and information of the enterprises, organizations, and individuals. This leaves the privacy of the user(s) more vulnerable to the attack. One of the very sensitive attacks is known as “Man-in-The-Middle Attack”.

[3] The phrase "Man-In-The-Middle" refers to a situation in basketball where 2 players are attempting to hand over the ball to one another as a third player seeks to intercept it. Attacks using MITM are often known as fire brigade or bucket brigade attacks. [4] These names come from the method used by the fire brigade to put out a fire by transferring buckets between individuals standing between the water source and the flames. TCP session hijacking, Session hijacking, TCP hijacking, and Monkey-in-the-middle attacks are other names for MITM attacks.

[5] Man-in-The-Middle attack is a common terminology for when an adversary keeps himself in between a conversation of 2 users through software application - either to impersonate or to eavesdrop on one of the two parties. [6] Typically, an MITM attack comprises a third party (attacker) and two endpoint devices (victims). The attacker already has control over the channel of communication between the two endpoints and can change the content sent across it.[7] The motive of an attack is for stealing personal sensitive data, such as credit-card details, bank-account details, and other data such as login credentials. The usage of this information gathered during an attack may include unauthorized fund transfers, identity theft, or unauthorized password changes.

[8] Using the DNS spoofing technique, the IP address returned by a client's repeated DNS queries can be changed to match the attacker's desired IP address. A Man-in-the-Middle attack should also be conducted in order for the DNS spoofing attack to be successful, and this can be done through ARP spoofing. A DNS spoofing attack's series of events can be summed up as follows: - Intercept all DNS requests -> Return faked IP addresses -> ARP spoof to connect attacker's computer physical address (MAC) to IP address of the gateway [9]. DNS spoofing works by taking advantage of the way regular DNS queries operate. DNS packets are UDP packets, and as such, they often don't provide any authentication or encrypted information to confirm the packet's legitimacy. Therefore, by taking advantage of the absence of authentication mechanisms, anyone can impersonate the DNS server. To link the L2 layer address to the L3 layer address, ARP spoofing is necessary.

2 Literature review

Ref No.	Work Done	Techniques used or Methods Described	Limitations or Future Work
1.	[1]In this re-	[1] This	[1]With this

- *Harshit Rastogi is currently pursuing bachelor’s degree program in Computer Science and Engineering in VIT University, India*
- *Dr. Krishnaraj N. is an Associate Professor Sr. in School of Computer Science and Engineering in VIT University*
- *Aravinth M is currently pursuing bachelor’s degree program in Computer Science and Engineering in VIT University, India*

	search, a method is provided to mitigate the aforementioned attacks by encrypting crucial data in messages and shielding them from tampering using an asymmetric cypher. The DNS server public key must be held by the client, and it can be acquired from the DNS server using either a static setup or a secure channel.	study creates private key and public keys for the DNS servers using the RSA algorithm as an asymmetric cipher. RSA is implemented using C language.	strategy, everybody can read the retaliation that is being sent ,but the main thing is that not everyone can decrypt the IP. Therefore for this paper, IP encryption is required for DNS server authentication.
2.	[2].This paper basically focuses mostly on how to understand the attack "men-in-the-middle attack. "The goal of this paper is to aid readers in comprehending and becoming familiar with the topic .	[2]There are various types of Man-in-the middle-attacks that have been described in this paper ARP SPOOFING,SSL ,CA Description, IP Spoofing and DHCP Spoofing.	[2]The report did not concentrate on in-depth analysis for Man-In-The Middle Attack future research directions.
3.	[3]This study used terms from penetration testing to conduct a security review on a website. The Man-In-The-Middle Attack technique is used to conduct this penetration test. This technique is still frequently employed by attackers who are not in control of sniffing, which involves tapping into a targeted machine to look for confidential data.	[3]The penetration testing techniques used in this research are basically-Cross-site scripting, SQL Injection, and Brute Force Attack	[3]The future work of this paper is basically to 1. Using the proper security system technique to prevent hacker intrusion. 2. When testing the MITM approach, employ methods other than sniffing.
4.	[4]The purpose of this paper is to clarify the MITM and its various categories. This paper's final goal is to propose some mechanisms for preventing such attacks.	[4]In this paper various techniques are given to detect the Man in the middle attacks such as Voting-based solutions, server-based and host-based solutions, and cryptographic solutions	[4]It is possible to combine man-in-the-middle attacks with a variety of cryptographic techniques, including key diffusion and elliptic curve cryptography. The study focuses to expand on this research in future work in order to assess the effects of such attacks in various VANET backgrounds using the adaptability of the nodes.
5.	[5]In some of the most important CPS (Cyber Physical Systems) domains, this article describes the security concerns facing CPSs . To understand the present situation of the hazards to CPS, investigate and analyse the dangers that have been mentioned in earlier studies and research.	[5]This study has basically described the tools through which we can get access to attacks, the vulnerabilities in the system that can make our system more prone to attacks, what are the results of those attacks along with the objectives. They have used several models like three tenets threat models to determine elements needed for the successful attack and also provide the various taxonomies.	[5]Organizations and researchers lack the ideas and tools necessary to comprehend the different trending risks and the consequences that every threat may have on the software systems. Future research will focus on the development, methods, applications, categories of assaults, analysis of security concerns, and current trends, and open research issues related to the cyber-physical security mechanisms.

			This will be done by examining the tools that can be used to stop hackers from improving the recovery systems and gaining access to these systems to reduce the impact of the attack.
6	[6]The classification of MITM attacks into different groups in this research is based on a number of different criteria. Execution steps for each MITM class based on impersonation strategies are presented. Finally, a classification of MITM prevention techniques was suggested.	[6]Classified MITM attacks using GSM and UMTS, two frequently used network technologies, as well as OSI, a reference model. The main proposed classes of MITM attacks are based on the location of the attacker and victim, the communication route, and the impersonation techniques..	[6]The limitations of this paper is that this paper did not cover MITM attacks in all communication channels. The major limitation of this paper is that it does not propose a solution for the new technologies such as RFID, LTE, SIP, HB-like, and VoIP. Also this paper only discussed the MITM attacks which have same traffic flow - traffic which goes through middleman. But the other models of MITM are also in existence.
7	[7]In this study, the viability of MITM attacks is evaluated using analysis and numerical data from the public Ethereum blockchain, a consortium, and private blockchains. In public, consortium, and private contexts, this article provided the fully realized assault against the Ethereum blockchain technology.	[7]This article describes significant topological characteristics of the Ethereum public blockchain. Additionally, VMs with limited CPU quantum were created, and the blockchain was evaluated for resistance to MITM attacks, BGP hijacking, and ARP spoofing. The findings showed that targeting Ethereum in a consortium or private setting is highly damaging. Then, a number of defences were put forth in an effort to lessen the vulnerability to MITM assaults.	[7]The proposed countermeasures are short-term. The demonstrated system when implemented over a WAN, the success rate of MITM attack and double spending is high.
8	[8]This paper proposed a system that detects and prevents the MITM attack that is happening through web portals using tokenization of the sessions between the client and the server.	[8]In this paper, the technique used is the process of binding the tokens of the session by making an identifier on the basis of a private key. The client generates a public and private key pair each time for every website that it needs to use a token on. The private key is kept secretly and checking is done against the identifier. The signature is on the public key and keying material of the contemporary Transport Layer Security (TLS) connection. A pseudo random number is added to the key pair and tokenized.	[8]The limitation in this paper is that it only proposes the method for the applications that use the sessions.
9	[9]In order to identify, isolate, and reconfigure victim systems	[9]The MITM-method IDS of identifying attackers is based	[9]This method detects the MITM attacks and is less likely

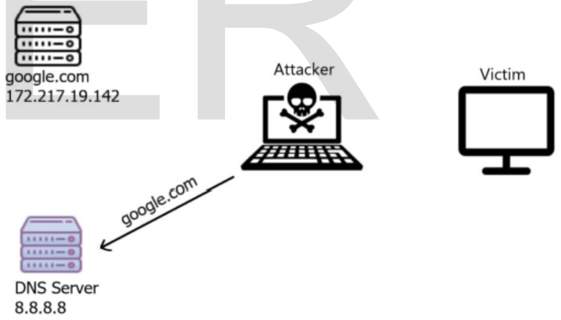
	in wireless sensor networks, this study suggests the Intrusion Detection System (MITM-IDS) concept. For handling MITM attacks, an IDS based on deep learning has been suggested.	on signature-ID templates. The proposed MITM-IDS operates through a network of centralized databases (CDN). Additionally, tools for packet sniffing and network intrusion detection systems (NIDS) are used. Long Short Term Memory (LSTM), among other techniques of machine learning, is also employed.	to prevent the attack. This system only isolates and reconfigures the victim nodes rather than preventing the attack from happening.
10	[10]This study examined the prevalence of networks that are susceptible to intrusion using fake addresses. Nearly 4000 DNS server instances that were vulnerable to cache poisoning attacks were also found during this research.	[10]Mainly used the technique called Destination-side Source Address Validation (DSAV). Tested a large number of DNS servers for various attack categories by taking a large data set. Techniques such as Source Port Randomization, OS Identification, Forwarding and Local System Infiltration are used.	[10]Investigated and analysed the attacks on many DNS servers but did not provide a strong alternative way to prevent the attack from happening.
11	[11]It has been shown that it is simple to attack HTTPS-secured Web connections by utilizing some standard LAN features as well as typical user behaviour. The assault is not easy to execute, but an experienced user will have no trouble doing it. Furthermore, the ease with which an attacker may create a fake certificate highlights the necessity for websites to be aware of the dangers of self-signed certificates.	[11]This article makes the assumption that a user on the client host (CH) wishes to conduct an HTTPS-encrypted transaction on the host server (SH). Given that CH, the attacker host (ATH) serves as a gateway for the traffic stream and SH must network exchange data. By intercepting communication at the source and sending it on to the target, the attacker gains the power to change and add messages covertly.	[11]Strong encryption is a useful tool for protecting data, but the level of security it offers depends on how strong the other encryption or weakest link is.
12	[12]This article explains a reliable method for defending the Diffie-Hellman protocol against man-in-the-middle attacks. The Geffe generator produced a binary sequence that was incredibly unpredictable. These sequences are also tested statistically before determining the private key and the shared key.	[12]The suggested approach makes sure that the private keys won't be transmitted over the channels and will instead be stored on the server as hashes. Because it can identify between the sender and the receiver on the basis of their user information, it also offers a non-repudiation feature. Our method thus provides additional security features than existing methods and protects against MITM attacks.	1[12]This method will be prioritized over other encryption techniques in this paper's future efforts to provide a secure cryptosystem for securely exchanging communications. The researchers will apply the suggested algorithm in a real cloud cryptosystem.
13	[13]Even when data is encrypted during data exchanges, there is a chance that others will discover the data. One possibility is that the person eavesdrops on the two people's communi-	[13]As a result of employing the interlock protocol to prevent man-in-the-middle attacks, the authors arrive at the conclusion that even if eavesdroppers were to get and replace the send-	[13]When the passwords are hashed, however, this is ineffective because only half of a hash is useful. Other approaches are also suggested, such as employing a shared secret in addition

	cation channel. This tactic is known as a Man-in-The-Middle attack. This study uses interlock protocols to protect communications from man-in-the-middle attacks while encrypting messages during transmission using the RSA method. Test results demonstrate that using interlock protocols can prevent man-in-the-middle assaults.	er's and receiver's public keys, they would not be able to access or alter communications. This is due to the fact that the encrypted communication is divided into two halves and delivered progressively, making it impossible for eavesdroppers to determine the original message that was sent.	to the password. The forced-latency improvement can help shield against some assaults.
14	[14]One of the most popular techniques used in network hacking is the Man-in-The-Middle attack. Attacks like Denial of Service (DoS) and port stealing can be successfully used by MITM attackers, which can have shockingly significant effects on customers in terms of both money loss and security issues. The traditional defence strategies focus on either how to identify and stop such assaults or how to stop them from ever being launched. In light of the fact that MITM attacks are unavoidable, this study offers a game-theoretic defence approach that tries to reduce the overall system's loss.	[14]We interpret the interaction between the attacker and the defender as a Stackelberg security game and use the Strong Stackelberg Equilibrium (SSE) as the defence's tactic.. In our model, the defender's strategy space is boundless, so we use a novel technique to condense the search space while determining the best defence plan. Finally, by contrasting our ideal defence approach with non-strategic defence techniques, we experimentally evaluate it. The findings show that, in terms of reducing overall losses from MITM attacks, our game-theoretic defence method performs noticeably better than alternative non-strategic protection strategies.	[14]Attackers target the actual data being exchanged between the endpoints, putting its integrity and confidentiality in danger. By intercepting communications and listening in on conversations, an adversary can put message integrity and confidentiality at risk. Additionally, an adversary may intercept, modify, or destroy messages to obstruct availability by preventing communication between two parties.

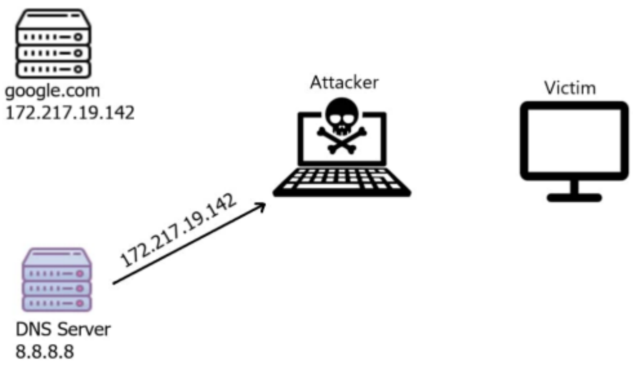
3.METHOD TO BE USED TO DO ATTACK

In order to change the IP address that appears in the DNS requests that are answered for the client, a series of actions must be taken. Here are the suggested actions that will be taken and the events that will take place for this attack to succeed:

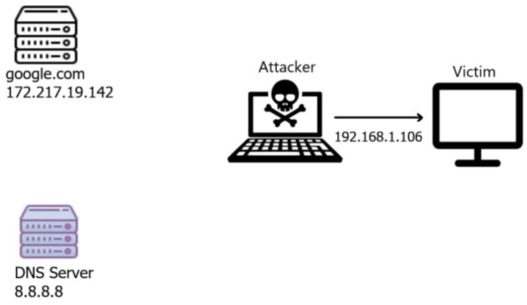
Due to his position in the middle, the attacker will get the DNS request requesting "what is the IP address of google.com," who will then submit it to the DNS server.



The DNS server will provide a DNS answer in response to a valid request.



Once the attacker has the DNS answer with Google.com's true IP address, they will change this IP address to a malicious fake IP.



4. TOOLS THAT CAN BE USED

1. Host Machine: Laptop or Desktop where virtual machines will be launched
2. Virtual Machine (Victim): Virtual Machine to be attacked
3. Virtual Machine (Attacker): Virtual Machine that will perform DNS spoofing on victim
4. Python 3.6: For writing DNS and ARP spoofing scripts
5. Apache server: To host the fake google webpage
6. NAT Network: Network of Virtual Machines (Victim, Attacker and other virtual machines)
7. Python Libraries (Scapy, NetFilterQueue): Used for packet processing.
8. VirtualBox (by Oracle): To create and manage virtual machines.

5. HOW TO PREVENT MAN IN THE MIDDLE ATTACK?

1. Prohibit using public networks for any private work by workers
2. Avoiding entering the passwords and sensitive data using Wi-Fi networks.
3. Noticing browser warnings and that a website is insecure and taking action on it.
4. When a secure application isn't in use, immediately log out.
5. Avoiding use of public Wi-Fi networks when carrying out transactions that are so important.
6. We can assist in preventing potential assaults by employing surfing encryption software to encrypt the traffic travelling between the network and your device.

6. DISCUSSIONS

DNS spoofing alters the DNS requests made by the clients. Man-in-the-Middle attack is also performed while spoofing the DNS. This is performed through spoofing the ARP. From surveying various researches made by many authors, this paper compiles methods and preventive measures to take in order to avoid such attacks. Many papers have analyzed the attacks and given many theoretical solutions. Few papers have done the demonstrations of the attacks and also given the solution mechanism to avoid the attacks. Many authors have given the solutions by including the various domains such as Machine Learning, Deep Learning and many more. The different networks such as LAN, WAN are analyzed and tested for the solution. The papers also have considered different communication channels and provided the solution for corresponding channels. New technologies such as RFID, LTE, SIP, HB-like, and VoIP are also tested for the attack and the vulnerabilities in these are mentioned and solutions are made.

7. CONCLUSION

A fundamental component of Denial-of-Service and Man-in-The-Middle assaults is a DNS attack. The attacker takes advantage of DNS messages sent in plain text to manage an attack. The suggested system requires little processing time to survive DNS attacks. The query ID and answer name server IP are the two key pieces of information that are encrypted by the proposed strategy using an asymmetric encryption technique. To protect the information from the attacker by authenticating the server, both parameters are needed. As a result, the attacker finds it difficult or impossible to guess the information. As a result of the approach of including the decrypted ID in the response to transmit, the results demonstrate that the suggested technique does not experience a denial of service since the query and response IDs are different. Going forward, we would like to explore remedial measures for such attacks and how to protect against them.

REFERENCES

[1] Hussain, M. A., Jin, H., Hussien, Z. A., Abduljabbar, Z. A., Abbdal, S. H., & Ibrahim, A. (2016, July). DNS protection against spoofing and poisoning attacks. In *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)* (pp. 1308-1312). IEEE.

[2] Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109-134.

[3] H. Poor, “A Hypertext History of Multiuser Dimensions,” *MUD History,* http://www.ccs.neu.edu/home/pb/mud-history.html. 1986. (URL link *include year)

[4] .Javeed, D., MohammedBadamasi, U., Ndubuisi, C. O., Soomro, F., & Asif, M. (2020). Man in the middle attacks: Analysis motivation and prevention. *International Journal of Computer Networks and Communications Security*, *8*(7), 52-58.

[5] Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2019). Review of cyber-attacks classifications and threats analysis in cyber-physical systems. *International Journal of Internet Technology and Secured Transactions*, *9*(3), 282-298.

[6] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, *18*(3), 2027-2051.

[7] Ekparinya, P., Gramoli, V., & Jourjon, G. (2018, October). Impact of man-in-the-middle attacks on ethereum. In *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)* (pp. 11-20).

IEEE.

[8] Krishnan, V. G., Kumar, B. A., Mohan, R., & Mohanasunder, V. (2020). Man in the Middle Attack Prevention using Token Generation Technique.

[9] Mohapatra, H., Rath, S., Panda, S., & Kumar, R. (2020). Handling of man-in-the-middle attack in WSN through intrusion detection system. *International journal*, *8*(5), 1503-1510.

[10] Deccio, C., Hilton, A., Briggs, M., Avery, T., & Richardson, R. (2020, October). Behind closed doors: a network tale of spoofing, intrusion, and false DNS security. In *Proceedings of the ACM Internet Measurement Conference* (pp. 65-77).

[11] Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy*, *7*(1), 78-81.

[12] Khader, A. S., & Lai, D. (2015, April). Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. In *2015 22nd international conference on telecommunications (ICT)* (pp. 204-208). IEEE.

[13] Rahim, Robbi. "Man-in-the-middle-attack prevention using interlock protocol method." ARPN J. Eng. Appl. Sci 12, no. 22 (2017): 6483-6487.

[14] Li, Xiaohong, Shuxin Li, Jianye Hao, Zhiyong Feng, and Bo An. "Optimal Personalized Defense Strategy Against Man-In-The-Middle Attack." In AAAI, pp. 593- 599. 2017.