Using Mininet Simulator to Develop Man in the Middle Attack Scenario

1st Keya Shah
Computer Science and Engineering,
University of North Texas,
Denton, Texas
KeyaAmishkumarShah@my.unt.edu

2nd Vrushabh Desai
Computer Science and Engineering,
University of North Texas,
Denton, Texas
VrushabhAjaybhaiDesai@my.unt.edu

3rd Gurpartap Singh
Computer Science and Engineering,
University of North Texas,
Denton, Texas
gurpartapsingh@my.unt.edu

***Abstract*—ARP is a protocol that transforms IP addresses into mac addresses and vice versa. People are growing increasingly reliant on the internet and using it to exchange personal information. If ARP can't find an IP address for a particular mac address, it looks for a similar mac address on the network. This type of opportunity is exploited by the attacker. This sort of attack is common, thus we're utilizing a mininet simulator to create a situation with several connections.**

***Index Terms*—ARP spoofing; ARP poisoning; MITM; Man in the Middle Attack; Mininet; ARP cache poisoning; mininet; attack scenario using mininet**

I. Introduction

In today's environment, using the internet is a significant concern. To connect to the internet, you can use either a cable or a wireless connection. Wireless internet access is more well-known than the others. As a result of gadgets' ability to interact with one another from everywhere on the earth, anyone can access the internet from anywhere. In order to connect to the internet, a wireless connection transmits a signal to the local area network. As a result, we are able to access the internet without the use of any type of cable. Every technological advancement, however, has a drawback. Attacking such a connection is also vulnerable to the attacker. A wired connection is difficult to attack since it is solely vulnerable to the environment to which the wires are attached. People are becoming more reliant on the internet and exchanging their personal information over it as the number of internet users grows. If an attacker succeeds in breaching their security, they will have access to all of their personal information, as well as their bank and other domain passwords. The attacker can utilize a variety of techniques, including the Man in the Middle attack, eavesdropping, phishing, and social engineering. The Man in the Middle, which may be utilized to attack, will be discussed in this study [1].

A man-in-the-middle attack can be carried out in ARP (Address Resolution Protocol). ARP is a network protocol that binds network messages to a specific network device. ARP essentially converts an IP address to a mac (Media Access Control) address and vice versa. If ARP is unable to locate an IP address for a given mac address, it searches the network for a similar mac address and records the information in the table. A table for each server displays which IP address corresponds to which mac address. Furthermore, because ARP is not intended for security, it does not verify if the IP address or mac address it discovers is legitimate. For example, if I fabricated the mac address for a certain IP address that ARP is looking for, I could act as the mediator, and all packets sent by that user would be routed via me. As a result, the attacker uses this method to get access to the network. Furthermore, attackers do not counterfeit addresses on only one side of the channel; they do so on both sides (sender and receiver). As a result, attackers may listen to a variety of information and make changes if they so choose. ARP spoofing, or ARP cache poisoning, is the term for this. This vulnerability, however, is only effective if the IP address is based on the IPv4 standard. IPv6 is safe and prevents users from forging addresses because it uses Neighbor Discovery Protocol (NDP). Despite this, the majority of networks employ the IPv4 protocol. As a result, this type of attack occurs often. Because the attacker listens to and may change all requests from the sender to the recipient and vice versa, this type of attack is known as a man-in-the-middle attack. [7] [8]

We'll look at man-in-the-middle attacks against the ARP protocol in this study. However, we won't be able to exhibit hundreds of networks on a single system. We'll use a mininet simulator to demonstrate the connections and see how data is digested in the network. Mininet is open-source software that allows users to combine many networks into a single simulator that can't be displayed on a single computer. [9]

II. Related Work

Numerous forms of attack scenarios or man-in-the-middle attack situations were explored and investigated in [2]. The hackers have utilized the BB84 protocol as a point of attack. As a result, in the BB84 protocol, communication between two peers is accomplished by exchanging a quantum cryptographic key. So, when messages are transmitted, or, in technical terms, when bits are exchanged, the Man In The Middle will try to detect the bits that were passed from one peer to another and modify them. Because they are cached, the attacker will replace the IP with its own neighboring MAC address and construct a bogus message to decode the information, allowing for eavesdropping. TCP SYN flooding is shown as a Man In The Middle attack in [3]. As a result, in this form of attack, an attacker would often send repeated SYN packets to all of the target server's ports, with the IP address for that being a

bogus one the majority of the time. Because the target server is unaware of the situation, it will respond to each attempt with an ACK, allowing the Man in the Middle to learn about the server's information and additional open ports. In our project, we'll use Mininet software, which is a simulator for building huge virtual connections or networks on a single system, in addition to the ARP protocol, and will attempt to intercept or fake the network's messages. Reference [4] shows a man-in-the-middle attack against ARP poisoning in wired connections is presented in this publication. The exploit was carried out via the Ettercap tool. IP address spoofing, DNS spoofing, and Gateway spoofing were all used in the Man in the Middle attack. So, in our project, we'll utilize the Mininet simulator to perform a man-in-the-middle attack against ARP spoofing, and the tool we'll use for the exploit will be Bettercap. In our project, we will employ the IP address spoofing approach, in which tables will be built for MAC addresses relating to their IP addresses, and the attacker will modify the IP address associated with the MAC address while executing the attack, allowing for eavesdropping

III. Methodology

We are leveraging the ARP protocol to create network attacks known as "Man In The Middle Attacks" (MITM). Because the ARP protocol is used to link IP addresses to their matching MAC addresses and store the addresses and their MAC addresses in a cache table. An attacker can try to eavesdrop on the system by attacking the cached table and learning the MAC address. They can then transmit a fake IP address to that MAC address. Mininet software or a simulator will be used to create large virtual connections on tiny or single hosts. So, because we require the IP address, we'll mostly focus on qualitative data, with some quantitative data thrown in for good measure, because the MAC address is made up of both numbers and words. Because we will be utilizing the live simulator to acquire the information, we have decided to use one main kind of data at this stage. As a result, the study will focus on the primary kinds of data, but at a later date, we'll see if the work can be done with datasets that are secondary to the types of data used to trigger the attacks or vulnerabilities. [10]

So, to acquire the data, we'll be employing a variety of technologies. We'll utilize tools like Mininet, which functions as a connection emulator, and then Bettercap, which is a program that captures an individual's data and is powerful enough to launch multiple Man In The Middle (MITM) attacks on the network. The attack's purpose is to obtain the MAC address or cache table information that the ARP protocol uses to transmit data packets across the network to the proper host. So, using these tools, we'll attempt to obtain data for a certain organization's communication system, and then try to spoof it by producing attacks. A victim who is transferring data via the network is classified as a person. With the use of these tools, an attacker will attempt to develop attacks and hack the system. In addition, bettercap, an open-source program used in ARP spoofing, is employed for data capture. To start Bettercap in a terminal, type "bettercap -iface" followed by the network interface where the assaults will take place. [11]

We will be using different tools like BetterCap and an emulator called Mininet. Once we have the data captured with us, we will try to import the data into any of the database tools with a preloaded template and check if the data collected is correct or not, whether in terms of syntax or any other technical glitch. [12] Similarly, when we have data with a mixture of alphabets and numbers, the analysis may be done for quantitative data. As a result, numerous limitations will be imposed on the scripts, which will be used to verify the type of data obtained in terms of syntax and other factors. When the victim uses the bettercap tool to transmit a packet and asks for the MAC address of the IP address it has, bettercap analyzes the IP address and always sends the victim its MAC address, leading the victim to believe that the address is valid and this is how the attack is carried out. [13]

So we'll try to create attacks on the network that uses the ARP protocol in conjunction with the IPV4 protocol. There have been a variety of alternative methods used to generate assaults or serve as "Man-in-the-Middle" attacks to hack the systems. Other methods include DNS spoofing, IP spoofing, HTTPS spoofing, and so on. These methods can also be used to attack the system, but because most people utilize the ARP protocol, there are more opportunities to attack the system. For example, if an attacker uses HTTPS spoofing to persuade you to redirect your website to a domain that does not have an SSL certificate but the victim is now aware of the attack, convincing him or her to switch to that website is tough. Other forms of outmoded limits exist as well. Some of them rely on outdated protocols, such as the BB84 protocol, which communicates via quantum cryptographic keys. Attacking the system through the ARP protocol, on the other hand, increases the likelihood of an attacker generating attacks. However, because we are using a simulator, there may be some limitations to this approach, it can only run in a linux-based system. On the other hand, it is very easy to create a large virtual environment, even small configuration systems, using virtual machines, so it is a cost-effective and even performance-wise more effective tool. Also, once we are linked to the victim's subnet, we will be able to obtain a large amount of data through the network from multiple systems.

IV. Experiments and simulation results

Using a mininet simulator [14], we're attempting to build a man-in-the-middle assault scenario. To do so, we must first install and set up the current stable version of the mininet simulator on the virtual machine. After installing the mininet, we'll set up the mininet simulator's network settings and construct a host-only adapter to link many workstations and generate the attack scenario. We're utilizing other virtual computers to join the mininet's single network, and then we're going to assault the machine. We can connect many computers to this network and log in to the virtual machines using a local server by establishing a host-only adapter. To connect to this

Fig. 1. ARP values before starting attack.

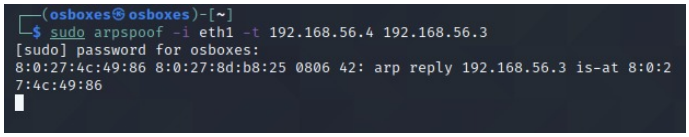

Fig. 2. Starting attack from the kali linux.

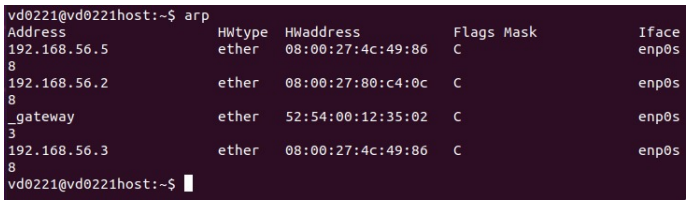

Fig. 3. ARP table values while under attack.

network, we must set up each virtual machine with a host-only adapter so that we can create a network scenario. We don't have a lot of machines in our study, so we're employing virtual machines to establish and join the same network. In real-world applications, however, all computers are connected to one another or to the internet [20] [21].

In this study, we used two virtual machines, Kali Linux and Ubuntu, to perform a man-in-the-middle attack, with Kali serving as the hacker's workstation and Ubuntu serving as the victim's machine. And we're snooping on traffic between Ubuntu and Mininet. As a server, we're utilizing mininet. To alter the arp table of Ubuntu from Kali Linux, we use the arpspoof application. The ARP table contains the various IP and Mac addresses of the computer to which they are linked. So, when the server and the victim start communicating, they first check for the mac address, as Ubuntu will say who has this specific IP address, and the server will respond that this mac address has a certain IP address connected. [15] After that, they can begin communicating with one another. Arpspoof is used to modify the mac addresses in this table. So, after altering the mac addresses of both machines, we can use Wireshark to simply observe traffic between them. We can see the data origin and destination IP addresses in Wireshark to confirm whether we intercepted the communication or not. We can also check this on an Ubuntu system by entering "arp," which will provide all IP and Mac addresses linked to Ubuntu. We may further verify the interception by looking at which IP address is associated with which mac address. Also, we tried to use the bettercap but it is not giving proper results so we changed the approach and used the arpspoof command [16].

We began by starting all three virtual computers, which included mininet, Kali Linux, and Ubuntu. Because Mininet is the server, all we have to do now is start it up so that other machines can connect to it. We attempted to connect to the mininet server using SSH from Ubuntu in order to obtain the IP address and Mac address of the mininet server. Connect to both computers using Kali Linux, in the same way, to retrieve entries in the ARP table. After that, we obtained the entries and disconnected all of the machines from that connection. [8] As indicated in the Fig. 1, the ARP table has a connection to the mininet server with the IP address 192.168.56.3, and we only need to take notice of the mac address. Then do the same thing with the mininet server and verify the client's mac address, which is Ubuntu (192.168.56.4). In the Fig. 2, from ubuntu to mininet communication. Then, to intercept traffic between the machines, we ran the arpspoof application. We used the command "arpspoof -i eth1 -t 192.168.56.4 192.168.56.3" to begin the spoofing. The letter "i" stands for the interface via which they are connected. All of the computers in this scenario are linked to "ethernet 1." And "t" stands for the target IP address, which is the IP address of the Ubuntu system. The gateway IP address, which is the server's IP address, is the final IP address. We've successfully intercepted Ubuntu and Mininet's conversations now. To double-check, we used an Ubuntu system and typed "arp" to get a list of all the IP and Mac addresses they're connected to. The same can be said for the server, which is mininet. As we can see in the Fig. 3, the mac addresses for both machines have been changed to the Kali Linux machine's mac address. [6]

We used the ARP spoofing application and also created an ARP spoofing Python script. ARP spoofing is described in the python script with numerous functionalities. We must first import scapy, a packet manipulation application. Users can send, sniff, and examine packets using it. We'll additionally import the time packets along with that. We defined the function for retrieving the system's mac address after importing the packets. In this function, we first created the ARP packet, then try to gather the mac address of the machine connected to the network, then use the scapy.srp function to send the ARP packets and it will wait for the ARP responses [17] [18] [19].

After that, we constructed a spoof function that gets the target's mac address, produces a malicious ARP response packet, and then sends it. When we wish to terminate the attack, we reassign the real IP addresses to the target device, so we write a restore function for it, which is similar to the spoof function developed previously, but the response packet sent here will be the system's real IP address.

Finally, we ran the entire script (Fig 4), and the attack occurred after a 2-second delay. Then when we want to terminate the execution of the script, we were able to press

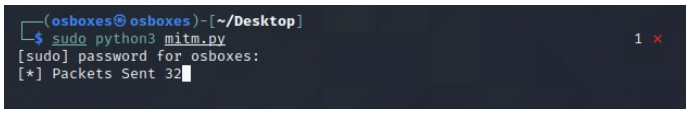

Fig. 4. ARP attack with python script.

the ctrl + C key on the keyboard to terminate the attack.

V. Conclusions

There are many tools and approaches for implementing the assaults often known as MITM (Man In The Middle Attack) have been explored in this article. We've utilized protocols like the ARP protocol, which is an address resolution mechanism that essentially transforms or converts an IP address to a MAC address and a MAC address to an IP address while also maintaining a table for the records, which is commonly referred to as the cache table. So, once an attacker gets information about the details of the above, he will try to spoof the IP address for the associated MAC addresses with a bogus address. We utilized a technology called mininet, which allows us to extract network information from a vast infrastructure onto a much smaller workstation. In addition, we utilized the famous Wireshark program to deceive the victim's IP address and MAC address. For the attack on the target, we used other workstations or versions of Ubuntu, such as KALI. We utilized the UNT CSCE Lab Image for Linux as the server and a mininet Linux system as the victim or client. We were able to manually create an attack by enabling the ARP and utilizing a Python script.

Although there are a variety of protocols and techniques that may be used to create MITM attacks, as well as a variety of countermeasures, the most crucial thing to remember is that the problem is within the protocol. As a result, the attacks may be carried out successfully due to protocol constraints. So, until and unless the protocol is abandoned, attacks are likely to occur. As a result, it is critical for an administrator to carefully consider the protocols that will be utilized and, if required, to take the appropriate steps to avoid these sorts of attacks.

References

[1] Amin, A.A.M. Mazharul, and Md Sadad Mahamud. An Alternative Approach of Mitigating ARP Based Man-in-the-Middle Attack Using Client Site Bash Script. 2019 6th International Conference on Electrical and Electronics Engineering (ICEEE), 2019. https://doi.org/10.1109/iceee2019.2019.00029.

[2] Huang, Jinxiang, Yong Wang, Huadeng Wang, Zhaohong Li, and Jinxiang Huang. Man-in-the-Middle Attack on BB84 Protocol and Its Defence. 2009 2nd IEEE International Conference on Computer Science and Information Technology, 2009. https://doi.org/10.1109/iccsit.2009.5234678.

[3] Huan-Rong Tang, Rou-Ling Sun, and Wei-Qiang Kong. Wireless Intrusion Detection for Defending against TCP Syn Flooding Attack and Man-in-the-Middle Attack. 2009 International Conference on Machine Learning and Cybernetics, 2009. https://doi.org/10.1109/icmlc.2009.5212317.

[4] Jami Manzoor1, Avinash Kumar2 and Sweety Kumari, ARP spoofing and Man in the Middle attack International Journal of Computer Engineering and Applications, Volume X, Special Issue, ICRTCST-2016 .http://www.ijcea.com/wp-content/uploads/2016/09/160314087.pdf

[5] Intro to ARP spoofing with bettercap. Æther Security Lab -. (n.d.). Retrieved April 16, 2022, from http://aetherlab.net/2016/02/intro-to-arp-spoofing-with-bettercap/

[6] Delgado, C. (2017, March 25). How to perform a man-in-the-middle (MITM) attack with Kali Linux. Our Code World. Retrieved May 11, 2022, from https://ourcodeworld.com/articles/read/422/how-to-perform-a-man-in-the-middle-mitm-attack-with-kali-linux

[7] Said, Y. (1968, January 1). ARP spoofing using a man-in-the-middle attack. in. Retrieved May 11, 2022, from https://tinyurl.com/5n89aez7

[8] The use of machine learning algorithms to detect man-in-the-middle (MITM) attack in User Datagram Protocol Packet Header. The Use Of Machine Learning Algorithms To Detect Man-in-the-middle (mitm) Attack In. (n.d.). Retrieved May 11, 2022, from https://researchjournali.com/view.php?id=5463

[9] An analysis of security solutions for ARP poisoning attacks and its effects on medical computing - researcher: An app for Academics. Researcher. (2019, November 14). Retrieved May 11, 2022, from https://www.researcher-app.com/paper/3879851

[10] (PDF) study on SDN with security issues using mininet. (n.d.). Retrieved May 12, 2022, from https://tinyurl.com/bdhbaktp

[11] Atlantis press. Atlantis Press — Atlantis Press Open Access Publisher Scientific Technical Medical Proceedings Journals Books. (n.d.). Retrieved May 11, 2022, from https://www.atlantis-press.com/

[12] Sukkar, G. A., Saifan, R., Khwaldeh, S., Maqableh, M., amp; Jafar, I. (2016, July 14). Address resolution protocol (ARP): Spoofing attack and proposed defense. Communications and Network. Retrieved May 11, 2022, from https://www.scirp.org/journal/paperinformation.aspx?paperid=68371

[13] Documentation. BetterCAP stable documentation. (n.d.). Retrieved May 11, 2022, from https://www.bettercap.org/legacy/

[14] Mininet. (n.d.). Mininet/mininet: Emulator for rapid prototyping of Software Defined Networks. GitHub. Retrieved May 11, 2022, from https://github.com/mininet/mininet

[15] International Journal Of Computer Engineering amp; Applications. (n.d.). Retrieved May 11, 2022, from https://www.ijcea.com/tag/httpwww-ijcea-comwp-contentuploads201606microsoft-word-n027-cameraready293-300-doc-pdf/

[16] Mallik, A. (n.d.). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi. Retrieved May 11, 2022, from https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453

[17] Usage - Scapy 2.4.5. documentation. (n.d.). Retrieved May 11, 2022, from https://scapy.readthedocs.io/en/latest/usage.html

[18] Python scapy.all.ether() examples. Python Examples of scapy.all.Ether. (n.d.). Retrieved May 11, 2022, from https://www.programcreek.com/python/example/86563/scapy.all.Ether

[19] Rockikz, A. (2019, July 29). How to build an ARP spoofer in python using Scapy. Python Code. Retrieved May 11, 2022, from https://www.thepythoncode.com/article/building-arp-spoofer-using-scapy

[20] Man-in-the-middle-attack: Understanding in simple words - research-gate. (n.d.). Retrieved May 12, 2022, from https://tinyurl.com/2s38mbkb

[21] Mininet. (n.d.). Mininet/mininet: Emulator for rapid prototyping of Software Defined Networks. GitHub. Retrieved May 11, 2022, from https://github.com/mininet/mininet