Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 7 Issue 8, August - 2020

Man-in-the-Middle Attack with WebSploit Tool

Füsun Yavuzer Aslan
Department of Computer Programming
Kırklareli University
Kırklareli, Turkey
fusunyavuzer@klu.edu.tr

Bora Aslan
(Corresponding author)
Department of Software Engineering
Kırklareli University
Kirklareli, Turkey
bora.aslan@klu.edu.tr

***Abstract*— If security measures are not taken in communication systems, attackers can easily obtain this information. In a communication system where security measures are not taken, attackers can listen to the messages sent, change them, send messages on behalf of someone else or use this message at another time by obtaining the sent message. One of the most desperate and dangerous attacks on the local network is a man-in-the-middle attack. With these attacks that violate the privacy policy of cyber security, all user information on the network can be captured.**

In this paper, it has been shown that Man-in-the-Middle attack can be done very easily by using the websploit tool in kali linux. The initiation of the attack is described in detail according to the given scenario. The moment of the attack was analyzed with the wireshark software. In the conclusion part, methods of protection from this type attacks are specified.

Keywords—Computer Networks, Information Security, Man-in-the-Middle Attack, MITM, ARP Poisoning

I. INTRODUCTION

MITM (Man-in-the-Middle) attack is one of the most well-known attacks in computing security which causes concern to security professionals, and is among the first hackers' eavesdropping attacks on the local network. The MITM attack is also used in the provisioning phase to initiate more complex attacks such as DoS and DNS spoofing. MITM attack is possible especially in a LAN environment where ARP poisoning can occur. At the end of these types of eavesdropping attacks, important users' data such as user ID, password, session information can be stolen [1].

WebSploit in Kali Linux operating system was preferred as the attack software. After the successful conclusion of the attack, MQTT and CoAP packets were analyzed with Wireshark software on the attacker computer.

II. ARP POISONING

In a local network environment, data transfer is carried out using MAC addresses. The MAC address operates at the data link layer of the TCP / IP protocol cluster. To communicate in a local network, it is important to convert the IP address to a MAC address.MAC addresses are 48 bits and IP addresses 32 bits.The protocol used to perform this process is called ARP (Address Resolution Protocol). When a device on the network wants to send data, it uses the ARP cache to find the MAC address of the receiving device, whose IP address it knows [2].

ARP packets in the TCP/IP stack are of two types, ARP request and ARP reply. When the sender device wants to know the MAC address of the target device to whom it wants to transmit data, sender device broadcasts the ARP request to every device on the network. The target device transmits the ARP reply packet to the sender device with unicast mode with the MAC address written in it. Once the reply packet is received, the receiver, that is sending the ARP request packet, caches the IP and MAC address mapping to speed up future communication. Under normal circumstances, all network devices communicate with the correct IP and MAC address by adhering to this systematic.

The ARP system has its own limitations. ARP does not perform any authentication, in other words, it does not test whether the IP-MAC address match is correct. On the other hand, ARP system does not prevent other devices on the network from sending an ARP response. Since there is no authentication check, the attacker can redirect network traffic to his or her own device in the same local network.

Under normal circumstances, all devices communicate with the correct IP and MAC address by adhering to this systematic. In this type of attack, the attacker sends a fake ARP reply packet claiming to have the IP address queried with the ARP request. Thus, fake IP address is saved in the cache of the requesting device. This process is called ARP poisoning. ARP poisoning allows all network traffic to be forwarded to the attacker's device.

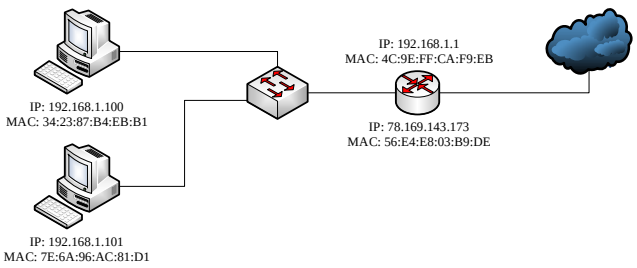


Fig 1: Sample Scenario for ARP Poisoning

In the Figure 1, devices with 192.168.1.100 and 192.168.1.101 IP addresses are connected to the WAN through a layer 2 switch via a gateway with an address of 192.168.1.1. When the computer with IP address 192.168.1.100 sends data to the external network, it creates the network packet and transmits it to the switch. The packet is transmitted through the switch to the router and from there to the external network. The direction of this data transmission is shown in Figure 2.

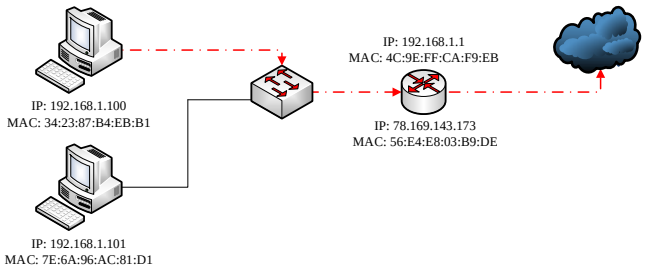


Fig. 2. Data Transmission before ARP Poisoning

Connected to the same local network, the attacker with IP address 192.168.1.34 initiates ARP poisoning and announces its MAC address as the gateway's MAC address to the local network. In this case, all devices connected to the network accept the attacker's device as a gateway and send all the packets that will be transmitted to the wide area network to the attacker. The attacker receives the packets, analyzes them, and then transmits them to the real gateway with IP address 192.168.1.1. The return of packets from the external network also occurs through the attacker. Victim devices that can communicate with the external network do not feel any disruption in the network. Data transmission after ARP poisoning is shown in Figure 3.

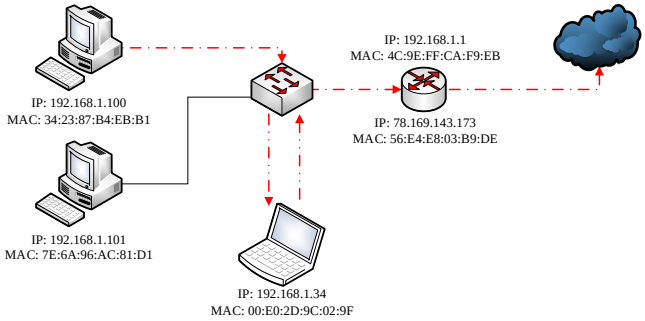


Fig. 3. Data Transmission after ARP Poisoning

After the ARP poisoning, the attacker can receive packets on the network and perform packet analysis, such as sniffing or spoofing.

III. MITM ATTACK WITH WEBSPLOIT

Kali Linux is an open source Debian-based Linux distribution which is developed and funded by Offensive Security. It provides services such as information security training and penetration testing. Kali Linux includes many tools for information security such as penetration testing, security vulnerability research, forensic informatics and reverse engineering. There are many tools for MITM attack in Kali Linux [3]. In this study, MITM attack was carried out using WebSploit. In addition, the packets on the network were analyzed with the Wireshark software.

WebSploit is an open source software developed in the python programming language used to scan and analyze the system to find various vulnerabilities. It includes many tools for ARP poisoning, sniffing HTTP traffic, scanning the network to detect devices on the network, scanning wireless networks, and creating fake wireless networks. WebSploit can be run with the **websploit** command on the console screen as shown in Figure 4.

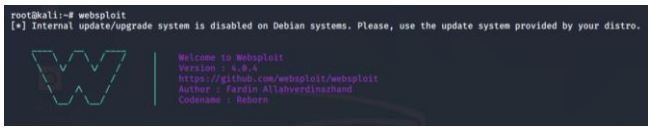


Fig.4 . Running the WebSploit

show or **show modules** command can be run on the console in order to see the tools in WebSploit and their explanations. There are 7 tools in 4.0.4 version. Some of these tools are used to scan the network and get information, while others are used for identity fraud. Attack tools in WebSploit are shown in Figure 5.

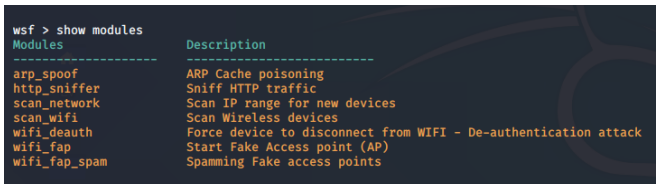


Fig.5 . Attack Tools in WebSploit

The **arp_spoof** tool in WebSploit is used to perform an ARP poisoning attack within a local network. To initiate ARP poisoning, the command **use arp_spoof** is run after WebSploit is started. Options command can be run to view the network's destination and gateway information. This process is shown in Figure 6.

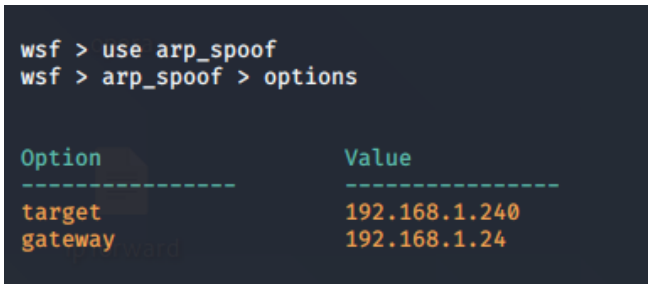
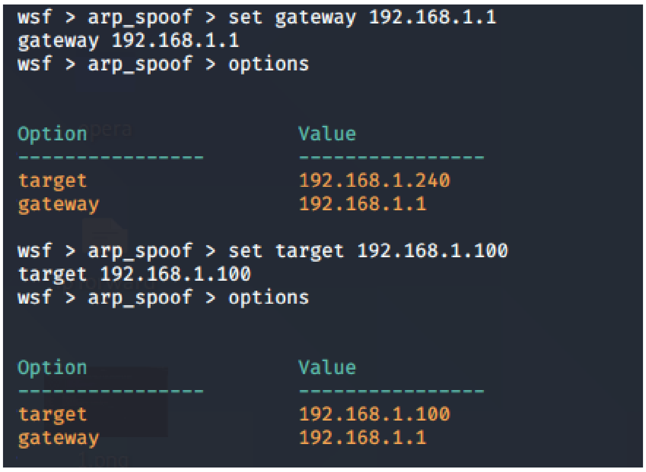


Fig. 6. **arp_spoof** Tool in WebSploit

The target and gateway IP addresses listed in Figure 6 are default values for WebSploit and should be set according to the network to be attacked by ARP poisoning. For this, **set gateway** and **set target**

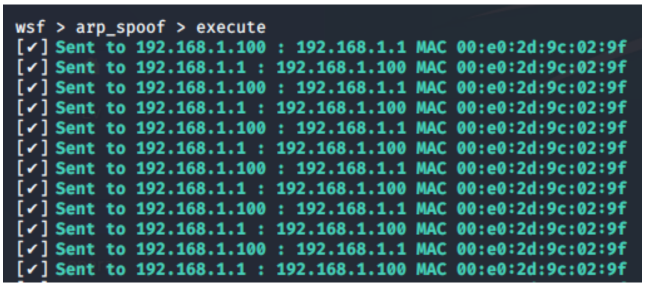
commands are used. According to the scenario given in Figure 3, Attacker with IP address of 192.168.1.34 wants to capture the traffic of the network and wants to listen to the traffic of the victim with IP address of 192.168.1.100. In this scenario, the attacker has to introduce himself/herself to the network as a gateway with IP address 192.168.1.1 and specify the computer with IP address 192.168.1.100 as the target in order to do ARP poisoning. The attacker sets the information of the network to attack with the commands **set target 192.168.1.100** and **set gateway 192.168.1.1** in the **arp_spoof** tool in WebSploit. This situation is given in Figure 7.



```
wsf > arp_spoof > set gateway 192.168.1.1
gateway 192.168.1.1
wsf > arp_spoof > options

Option                  Value
----------------        ----------------
target                  192.168.1.240
gateway                 192.168.1.1

wsf > arp_spoof > set target 192.168.1.100
target 192.168.1.100
wsf > arp_spoof > options

Option                  Value
----------------        ----------------
target                  192.168.1.100
gateway                 192.168.1.1
```

Fig. 7. Adjusting Information in WebSploit for ARP Poisoning Attack

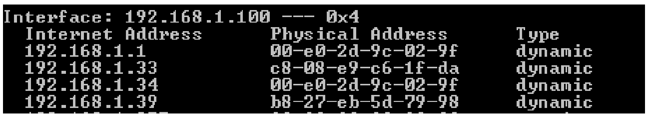
After the necessary adjustments are made, the attacker starts the ARP poisoning attack with the **execute** command in the arp_spoof tool in WebSploit as in Figure 8. Once the attack begins, the attacker fills the victim's ARP cache table by sending ARP packets to the target indicating the attacker is the gateway and completes the poisoning process. After that, the victim will send and receive network packets over the attacker's device in all data communication.



```
wsf > arp_spoof > execute
[✓] Sent to 192.168.1.100 : 192.168.1.1 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.1 : 192.168.1.100 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.100 : 192.168.1.1 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.1 : 192.168.1.100 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.100 : 192.168.1.1 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.1 : 192.168.1.100 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.100 : 192.168.1.1 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.1 : 192.168.1.100 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.100 : 192.168.1.1 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.1 : 192.168.1.100 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.100 : 192.168.1.1 MAC 00:e0:2d:9c:02:9f
[✓] Sent to 192.168.1.1 : 192.168.1.100 MAC 00:e0:2d:9c:02:9f
```

Fig. *8*.Starting the ARP Poisoning Attacks

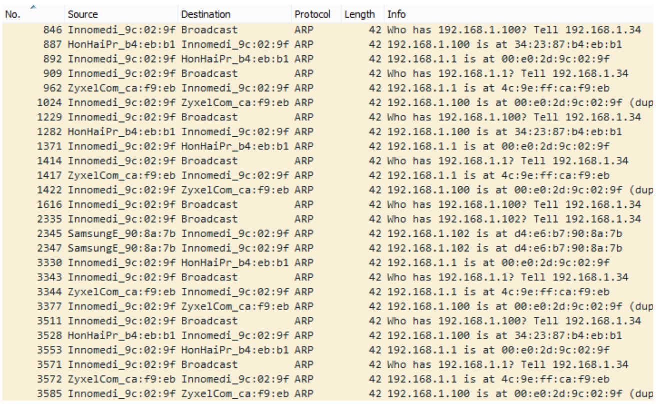
In the ARP poisoned network, the target computer's ARP cache table can be accessed with the **arp –a** command in the console. The victim's cache table is given in Figure 9. Accordingly, when the figure is examined, it can be seen that the MAC address of the attacker with the IP address 192.168.1.34 and the gateway with the IP address 192.168.1.1 is the same. In other words, the attacker revoked all protocol rules of the local network and forced himself onto the target computer as a gateway.



```
Interface: 192.168.1.100 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.1           00-e0-2d-9c-02-9f     dynamic
  192.168.1.33          c8-08-e9-c6-1f-da     dynamic
  192.168.1.34          00-e0-2d-9c-02-9f     dynamic
  192.168.1.39          b8-27-eb-5d-79-98     dynamic
```

Fig. *9*. ARP Cache Table of the Target Device

In Figure 10, some of the ARP packets during the ARP poisoning attack of the local network are analyzed and listed by Wireshark software. First of all, in packet number 846, the attacker queries the MAC address of the target with IP address 192.168.1.100 with the ARP request packet. Due to TCP/IP rules, the victim responded to this request with an ARP reply packet and sent the 887 packet. In the next step, with the 892 packet, the attacker communicates to the victim that the gateway with IP address 192.168.1.1 matches its own MAC address. In addition, the attacker transmitted to the whole network with the ARP request packet that he wanted to learn the MAC address of the local network gateway with the 909 numbered packet, and the gateway responded to this request with the 962 packet to send the MAC address to the attacker. With the 1024 packet, the attacker conveyed to the gateway that the IP address 192.168.1.100 belongs to him in order to receive the packets that will be sent to the victim. In the meantime, although the gateway states that the 192.168.1.1 IP address is conflicting, the MAC address-based communication operating at the data link layer is not broken. With this way, the ARP poisoning attack continues until the target devices' ARP cache is full. As a result, network traffic is unavoidably provided by flowing over the attacker, and the MITM attack is successful.



No.	Source	Destination	Protocol	Length	Info
846	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.100? Tell 192.168.1.34
887	HonHaiPr_b4:eb:b1	Innomedi_9c:02:9f	ARP	42	192.168.1.100 is at 34:23:87:b4:eb:b1
892	Innomedi_9c:02:9f	HonHaiPr_b4:eb:b1	ARP	42	192.168.1.1 is at 00:e0:2d:9c:02:9f
909	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.34
962	ZyxelCom_ca:f9:eb	Innomedi_9c:02:9f	ARP	42	192.168.1.1 is at 4c:9e:ff:ca:f9:eb
1024	Innomedi_9c:02:9f	ZyxelCom_ca:f9:eb	ARP	42	192.168.1.100 is at 00:e0:2d:9c:02:9f (dup
1229	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.100? Tell 192.168.1.34
1282	HonHaiPr_b4:eb:b1	Innomedi_9c:02:9f	ARP	42	192.168.1.100 is at 34:23:87:b4:eb:b1
1371	Innomedi_9c:02:9f	HonHaiPr_b4:eb:b1	ARP	42	192.168.1.1 is at 00:e0:2d:9c:02:9f
1414	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.34
1417	ZyxelCom_ca:f9:eb	Innomedi_9c:02:9f	ARP	42	192.168.1.1 is at 4c:9e:ff:ca:f9:eb
1422	Innomedi_9c:02:9f	ZyxelCom_ca:f9:eb	ARP	42	192.168.1.100 is at 00:e0:2d:9c:02:9f (dup
1616	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.100? Tell 192.168.1.34
2335	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.34
2345	SamsungE_90:8a:7b	Innomedi_9c:02:9f	ARP	42	192.168.1.102 is at d4:e6:b7:90:8a:7b
2347	SamsungE_90:8a:7b	Innomedi_9c:02:9f	ARP	42	192.168.1.102 is at d4:e6:b7:90:8a:7b
3330	Innomedi_9c:02:9f	HonHaiPr_b4:eb:b1	ARP	42	192.168.1.1 is at 00:e0:2d:9c:02:9f
3343	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.34
3344	ZyxelCom_ca:f9:eb	Innomedi_9c:02:9f	ARP	42	192.168.1.1 is at 4c:9e:ff:ca:f9:eb
3377	Innomedi_9c:02:9f	ZyxelCom_ca:f9:eb	ARP	42	192.168.1.100 is at 00:e0:2d:9c:02:9f (dup
3511	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.100? Tell 192.168.1.34
3528	HonHaiPr_b4:eb:b1	Innomedi_9c:02:9f	ARP	42	192.168.1.100 is at 34:23:87:b4:eb:b1
3553	Innomedi_9c:02:9f	HonHaiPr_b4:eb:b1	ARP	42	192.168.1.1 is at 00:e0:2d:9c:02:9f
3571	Innomedi_9c:02:9f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.34
3572	ZyxelCom_ca:f9:eb	Innomedi_9c:02:9f	ARP	42	192.168.1.1 is at 4c:9e:ff:ca:f9:eb
3585	Innomedi_9c:02:9f	ZyxelCom_ca:f9:eb	ARP	42	192.168.1.100 is at 00:e0:2d:9c:02:9f (dup

Fig. 10. ARP Packets during an ARP Poisoning Attack

IV. CONCLUSION

Man in the middle attack is an attack method that includes listening to the communication between two connections and capturing various data or listening to the communication, but also making any changes. With this attack it is possible to capturing and manipulating packets on the network. In this study, it

has been shown that this dangerous attack how can be done easily with a few simple tools.

There are some methods to prevent ARP poisoning or to ensure safety. Some of these methods can be listed as follows:

- Using static MAC address,
- Using VPN,
- Using controlled package analysis,
- Using Encryption.

Some of these methods place serious workload on system administrators. For example, mapping devices with static IP and MAC addresses can partially prevent such attacks however making it difficult to manage, especially in large networks. On the other hand, attacks can be prevented by detecting anomalies in network traffic with some packet analysis and filtering software. However, this may cause a noticeable slowdown in network traffic. Using VPN can be offered as another solution, but this adds to cost and complexity. As another solution, it is possible to use secure protocols such as HTTPS and SSL in the network. Of course, this solution will increase the cost, especially in large networks. One of the best and cost-effective solutions that can eliminate this security problem in the network environment can be considered as the encryption of packets in order to ensure the safe transmission of data without changing the operation of the network.

REFERENCES

[1] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys and Tutorials, 18(3), 2027-2051.
[2] Forouzan, B. A. (2009). TCP/IP protocol suite 4 edition: McGraw-Hill, Inc.
[3] Najera-Gutierrez, G., & Ansari, J. A. (2018). Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd.
[4] https://github.com/websploit/websploit
[5] https://www.wireshark.org/