A simple detection tool to detect man-in-the-middle attack in LANs

Haimashreelakshmi (212IS010)

Department of Computer Science and Engineering
National Institute of Technology Karnataka
Surathkal, Mangaluru, India

Abstract. Man in the middle(MITM) is a attack which is used by hacker to get infromations communicated between two nodes in network.There are many ways to perform this attack and one among them is Adress resolution protocol (ARP) spoofing/poisoning.This method is used by attacker to perform MITM attack in LANs.This attack is very simple to perform but its very dangerous at the same time. Sensitive informations such as credit card details, passwords etc are stolen by hackers using this method. Large organizations are not exposed to this attack as they have very good network infrastructure. But small organizations or individuals are often exposed to this attack.In this paper various methods to detect ARP spoofing/poisoning are studied and simple and fast detection tool to detect MITM attack in LANs is developed.

Keywords: MITM attack, ARP spoofing/poisoning, LANs, Detection

1 Introduction

Man in the middle is a attack where two parties which communicate with each other think that they are directly communicating with each other but attacker has inserted himself between them and steals all informations sent between two parties.One example for this is eavesdropping.Here attacker makes connections with both parties independently and sends messages to them so that they believe that they are speaking with each other on private connection where as conversation is entirely under attackers control.
ARP protocol is a stateless protocol that is used by hosts in the network to get Media Access Control(MAC) address of the destination if its Internet Protocol(IP) address is known.Evert host maintains ARP cache/table that has IP to MAC mapping which is used to connect to destination machine in the network.If host doent know MAC of certain machine then it sends ARP request packet to all machines in the network with destination IP address. Destination machine does not verify whether this is from authorized party or not. Also it allows all hosts to accept reply even if it has not raised any request. This is drawback od ARP protocol which is used by attacker to get control over host.

1.1 Problem Description

MITM attack is one of the major attack in LANs which causes various types of security issues.Study on this attack caused by ARP spoofing and its various detection techniques is done and simple and realiable tool to detect MITM attack through ARP spoofing is implemented.

1.2 Motivation

Large organizations have very secure network infrastructure beacuse of which they are safe from MITM attack through ARP spoofing.But LAN users are often exposed to this threat.There must be some simple and fast detection tool to detect this attack in LANs.

1.3 Scope

The detection tool developed can be used by LAN users to detect if they are under MITM attack or not.

1.4 Objectives

1. Study on various MITM attacks based on ARP spoofing.
2. Understanding various detection techniques to detect this attack.
3. Design a simple tool to detect MITM attack.

1.5 Organization of the Report

The next part of this report consists of literature survey as section 2, proposed approach as section 3, experimental results as section 4 and finally a conclusion.

2 Related Work

In this paper various types of MITM attacks are studied by considering OSI, GSM and UMTS reference models. These attacks are classified based on location of attacker, the communication channel used and impersonation techniques [1]. Existing measures against these attacks are studied and comparison is made between them [1]. Nayak GN et al. made a study on different MITM attacks and solutions possible for these attacks so that user can adopt these to prevent attacks [2]. A detail study is also done on ARP spoofing which is used by attacker to do MITM attack.
Bhushan et al. discussed about MITM attacks in wireless networks, weaknesses leading to this attack and how to take care to prevent this attack [3]. Abad et al. made a study on various schemes available to detect ARP cache poisoning is studied based on its strength and weakness [4]. Requirements for ideal solution is also proposed here. In the paper by Ponpat et al. ARP cache mapping is

replicated and stored in long-term application memory [5]. This is checked periodically against ARP cache maps to identify changes and to take appropriate actions.
Shukla et al. proposed solution for ARP spoofing by automatically configuring static ARP entries [6]. The results of this method tells that it can block any attacker in few microseconds under heavy traffic [6]. Jaideep et al. studied various types of poisoning with respect to ARP. Various detection and prevention methods and studied and compared [7]. In the paper published by Trabelsi et al. instead of stateless ARP cache, stateful ARP cache is used. Novel fuzzy logic is used to differentiate between normal and attackers ARP replies [8]. This fuzzy logic uses dynamically created database that adapts to network changes [8].
The paper by Nam et al. proposed enhanced version of ARP protocol. If the machine knows correct MAC address for given IP then if it doesn't remove this IP until machine is alive then no attack is possible using this IP. In order to prevent MITM attack even for a new IP address, we propose a new IP/MAC mapping conflict resolution mechanism based on computational puzzle and voting [9]. In the paper published by Mangut et al. evidences captured before attack is compared with evidences captures when network is under attack to evaluate proposed tools to detect ARP spoofing attack [10]. To mitigate the ARP poisoning attack, the security features DHCP Snooping and Dynamic ARP Inspection (DAI) are enabled and configured on a Cisco switch [10].

3 The Proposed Approach

In the proposed system first attack is done on victim's machine using attacker machine and then ARP table of victim's machine is used inorder to detect this attack.
To do this first find IP of target machine and gateway.Then open kali linux and give following command in root terminal to modifies ARP table of target machine.
$arpsoof - ieth0 - t[targetIP][gatewayIP]$
To modify ARP table of gateway give following command in root terminal.
$arpsoof - ieth0 - t[gatewayIP][targetIP]$
Now if ARP table of target machine is seen then we can find that MAC address of gateway is same as MAC address of attacker.By doing these changes attacker ensures that whatever packet is transferred between target and gateway always passes through attacker.
In this project python language script is used to detect these changes in ARP table to check if MITM attack is done or not.ARP table of the machine for which we want to check for MITM attack id retrieved using get_arp_table() given in Fig 1.

```
def get_arp_table(IP):
    cmd = "arp -a"
    process = subprocess.Popen(cmd, stdout=subprocess.PIPE, stderr=None, shell=True)
    output = process.communicate()
    interfaceBlocks = output[0].decode().split('Interface:')

    for interfaceBlock in interfaceBlocks:
        lines = interfaceBlock.split('\r\n');
        interfaceIP = lines[0].split('---')[0].strip()

        if interfaceIP == IP:
            names = ['Internet Address', 'Physical Address', 'Type']
            reader = csv.DictReader(
                lines[1:], fieldnames=names, skipinitialspace=True, delimiter=' ')
            next(reader)

            return [block for block in reader]
```

Fig. 1. Get ARP table of machine

IP address of the machine on which code is run is obtained using get_ip() function defined in Fig 2.

```
# Get IP Address
def get_ip():
    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    try:
     # doesn't even have to be reachable
     s.connect(('10.255.255.255', 1))
     IP = s.getsockname()[0]
    except:
     IP = '127.0.0.1'
    finally:
     s.close()
    return IP
```

Fig. 2. Get IP address of target machine

In the main part of the code these two functions are used to get IP and ARP table of machine.mac_address stores MAC of gateway.If this is same as any other machine MAC address then that means gateway is attacked by that machine. Because MAC addresses are unique within the LAN.

```
IP = get_ip()
print("IP of victim machine is:",IP)
arp_table=get_arp_table(IP)
mac_address=arp_table[0]['Physical Address']
mitm = False
print("Gateway's MAC Address is:", mac_address, "\r\n")
print("Looking if there is MITM attack possible....")
for line in arp_table[1:]:
    if line['Physical Address'] == mac_address:
        mitm = True
if mitm:
    print("MITM Attack is Detected")
else:
    print("No MITM Attack Right Now")
```

Fig. 3. ARP table is monitored to check for MITM attack

4 Experimental Results and Analysis

In this project winodws 10 is taken as victim machine and kali linux as attacker machine.Initially ARP table of winodws 10 machine is obtained aa given in Fig 4. Here windows 10 as IP 192.168.223.165 and gateway as IP 192.168.223.70. Kali linux machine as MAC address of 08-00-27-95-bd-54.

```
C:\Users\Haimashreelakshmi>arp -a

Interface: 192.168.223.165 --- 0x6
  Internet Address      Physical Address      Type
  192.168.223.70        8a-1d-00-ec-46-ba     dynamic
  192.168.223.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Fig. 4. ARP table of windows 10 machine

Once the default gateway address is obtained from ARP table, using kali linux ARP spoofing is performed. First windows 10 machine is taken as target machine and then gateway IP address and arpsoof command is run to change ARP table of windows 10 machin in Fig 5. Then gateway is taken as target and windows 10 machine's IP as gateway in the command is run to change ARP table of gateway in Fig 6.

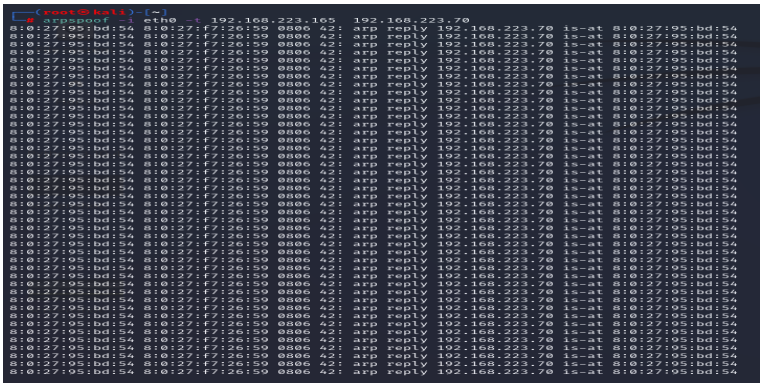

Fig. 5. ARP spoofing is done for winodws 10 using kali linux as attacker machine to change ARP table of windows 10

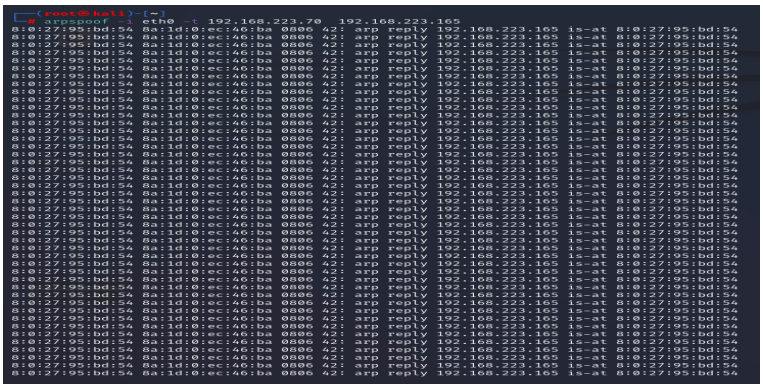

Fig. 6. ARP spoofing is done for winodws 10 using kali linux as attacker machine to change ARP table of gateway

Now if the ARP table of winodows 10 is displayed then MAC of gateway is changed to MAC of kali linux machine as given in Fig 7. Whatever packet is passed by windows 10 machine now through gateway its now passed through kali linux machine.So without knowlege about the attack winodws 10 machine shares its sensitive informations to the attacker.

```
C:\Users\Haimashreelakshmi>arp -a

Interface: 192.168.223.165 --- 0x6
  Internet Address      Physical Address      Type
  192.168.223.70        08-00-27-95-bd-54     dynamic
  192.168.223.213       08-00-27-95-bd-54     dynamic
  192.168.223.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Fig. 7. ARP table of windows 10 machine is changed after attack

This attack is detected by the code by running it on the victim's machine as given in Fig 8. It monitors ARP table of victim's machine and finds out about the MITM attack done on the machine.

```
MAN IN THE MIDDLE ATTACK DETECTION TOOL
IP of victim machine is: 192.168.223.165
Gateway's MAC Address is: 08-00-27-95-bd-54

Looking if there is MITM attack possible....
MITM Attack is Detected
```

Fig. 8. Program output

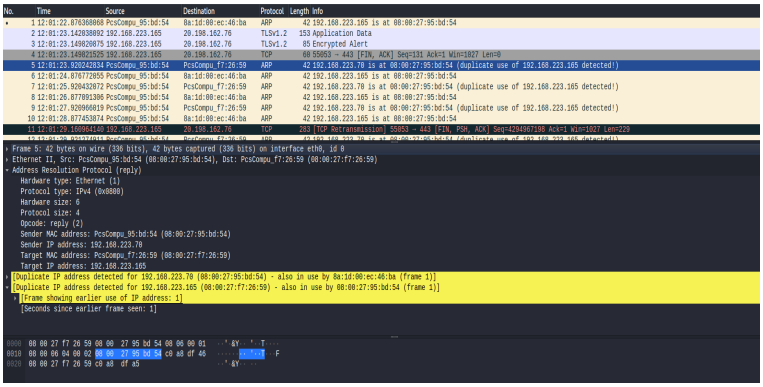

Fig. 9. ARP spoofing is analyzed using wireshark tool

5 Conclusion

The project is useful to detect MITM attack in LANs which is done through ARP spoofing.Study is done on how ARP aoofing takes places in LANs using kali linux and then using python simple code is written to detect MITM attack by monitoring ARP table of machine.
As a future work, MITM attack detection tool for WANs can be designed.This method must be simple and efficient enough than existing methods.

References

1. Conti M, Dragoni N, Lesyk V. :A survey of man in the middle attacks. IEEE Communications Surveys Tutorials. 2016; 18(3): 2027-2051.
2. Nayak GN, Samaddar SG. : Different flavours of man-inthe-middle attack, consequences and feasible solutions. 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. (ICCSIT). 2010, 5: 491-495.
3. Bhushan, B, Sahoo G, Rai AK. :Man-in-the-middle attack in wireless and computer networking; A review. 3rd International Conference on Advances in Computing, Communication Automation (ICACCA) (Fall). 2017:1-6.
4. Abad LC, Bonilla RI. : An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks. 27th International Conference on Distributed Computing Systems Workshops. 2007, 60: 60-67.
5. Ponpat Phetchai, Jema David Ndibwile, Doudou Fall, Shigeru Kashihara, Suppawong Tuarob. :Securing low-computaional-power devices against ARP spoofing attacks through lightweight android application. The 21st International Computer Science and Engineering Conference, 2017.
6. Shukla S, Yadav I. An innovative method for detection and prevention against ARP spoofing. International Journal of Computer Science and Information Technology Security. 2015; 5(1): 207-214.
7. Jaideep Singh, Vinit Grewal. :A Survey of Different Strategies to Pacify ARP Poisoning Attacks in Wireless Networks. International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 11, April 2015.

8. Trabelsi Z, El-Hajji W. :Preventing ARP attacks using a Fuzzy-based Stateful ARP Cache. IEEE International Conference on Communications. 2007, 1355-1360.
9. Nam SY, Kim D, Kim J. :Enhanced ARP: Preventing ARP poisoning-based man-in-the-middle attacks. IEEE Community Letters. 2010, 14(2):187-189.
10. Mangut AH, Al-Nemrat A, Benzaid C, Tawil ARH. :ARP Cache Poisoning Mitigation and Forensics Investigation. IEEE Trustcom/BigDataSE/ISPA. 2015, 1: 1392-1397.