www.ijecs.in
International Journal of Engineering and Computer Science
Volume12 Issue 05, May2023, PageNo.25717-25721
ISSN:2319-7242DOI: 10.18535/ijecs/v12i01.4671

Computer Network: An Implementation of MAC Spoofing

Mr. Lalit Jain
Senior Lab Assistant, Computer Science and Engineering, IIT Indore
lalit@iiti.a.cin

Abstract:
An exponential growth has observed of network or internet users due to diverse resource and information sharing services. Contrary, network uses also increased in different kinds of attacks. Means network is vulnerable for many types of attacks. Computer network may exploit in different contexts such as denial of service, ping death, malfunction routing, flooding, man in the middle and spoofing attack. Among of these mac spoofing is kind of attack spoofing attack that target to mac or physical address of the network host or router. It tampers original address to any other random or user defined address. The aim of the study is to present mac address and its types. With this, mac spoofing attack also presented. Implementation environment and method for the mac spoofing also presented. Mac spoofing is implemented in the kali linux operating system with the help of macchanger tool.

Key Words : Computer Network, Mac Address, Mac Address Types, Mac Spoofing, Kali Linux, Macchanger Tool.

1-INTRODUCTION

The motive of the network is to data exchange and resource sharing [1]. Today, resource sharing has significant market demand in term of cloud services. Inversely, use computer network or exploitation of network also growing. In network, communication accomplish through implementation of layered architecture or model. TCP/IP is popular for the communication of network entities [1]. TCP/IP is comprising of five layers such as application, transport, network, data link layer and physical layer which works for the different purpose. TCP/IP model is depicted in the fig-1.

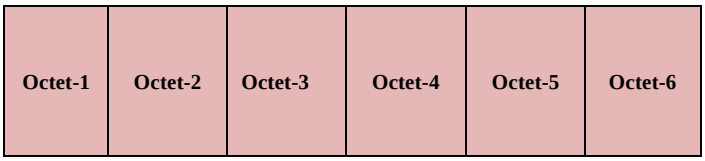
Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Fig-1: TCP/IP model

A computer or host in network environment has several addresses such port address, IP address or logical address as well as MAC or physical address [2]. Each type of address has some significance during the communication. On the other side the address also targets for the attackers. Attackers use these address to exploits network host or network router or firewall. In this work, we address significance of MAC address and how MAC address may be spoofed or changed by the attackers. Further, section presents MAC address, MAC spoofing, related study, attack environment and discussions.

Medium Access Control (Mac) Address

In the computer network, medium access control (MAC) address is physical address of network adapter or NIC that denoted with the help of hexadecimal numbers [3]. MAC addresses also known as Ethernet or LAN address. It is 48 bits long that written in 6 octets. Eight (8) bits used in each octet. First three octet of MAC address represents organization universal identifier (OUI) and last three octets represents device address identifier. The representation of MAC address is depicted in the fig-2.



Address Identifier

Fig-2: MAC Address Notation

Oui

An example of mac address is shown below.

A1: bc: 2f:31:b1:ca

Further mac address is classified in the following types [3]:

A. Unicast mac address

A mac address is said to be unicast, if least significant bit of first octet of mac address is 0.

Aa: 1c: 5d: 20:11: ba

As an example, above mac address is unicast address be

Cause fist octet is aa in hexadecimal that binary representation is 10101010. In the binary representation, least significant bit of aa is 0. For this reason, we can say given address is unicast mac address.

B. Multicast mac address

A mac address is said to be multicast, if least significant bit of first octet of mac address is 1.

Ab: 10: 2a: 2f:11: 1c

As an example, above mac address is multicast address because fist octet is ab in hexadecimal that binary representation is 10101011. In the binary representation, least significant bit of ab is 1. For this reason, we can say given address is multicast mac address.

E. Broadcast mac address:

Mac address or physical address of network host may be exploits by the attacker. When attackers able to change the actual or original mac address

I. Mac spoofing

Ab: 10: 2a: 2f:11: 1c

An example of mac address is shown below.

A1: bc: 2f:31:b1:ca

Further mac address is classified in the following types [3]:

C. Unicast mac address

A mac address is said to be unicast, if least significant bit of first octet of mac address is 0.

Aa: 1c: 5d: 20:11: ba

As an example, above mac address is unicast address because fist octet is aa in hexadecimal that binary representation is 10101010. In the binary representation, least significant bit of aa is 0. For this reason, we can say given address is unicast mac address.

D. Multicast mac address

A mac address is said to be multicast, if least significant bit of first octet of mac address is 1.

A mac address is said to be broadcast, if all bit of all octets of mac address is 1.

Ff: ff: ff: ff: ff:ff

As an example, above mac address is broadcast address because each octet is ff in hexadecimal that binary representation is 11111111. In the binary representation, all bits of each octet is 1. For this reason, we can say given address is broadcast mac address.

of machine then it is referred as mac spoofing. Further section addressed mac spoofing.

Mac spoofing is an art of changing mac address of

host in network environment. It is committed by the attackers to prevent physical attacking machine in the network environment. In other way, attacker also can change MAC address of victim and redirect sending data from the victim to another host.

- To bypass network security policies based on MAC address like bypass MAC filtering for accessing WIFI or its services.

MAC spoofing commits in the following ways:

- An attacker finds or identify victim or target MAC address that want to change. It can be happened by the scanning of network.
- Once target MAC address have identified, attacker may change their device address with target MAC address. It can be change either in random number or manually.

There are following motives for them MAC spoofing committed.

- Un-authorized access of network or its resources is motive to commits MAC spoofing.

- MAC Spoofing may also lead other kinds of attacks such as session hijacking, ARP Spoofing, Network eavesdropping and many more.

Next section presents, some research on MAC spoofing and its detection and preventions.

II. Literature Survey:-

There are some works have presented that addressed

There are some works have presented that addressed countermeasures and prevention procedure against MAC Spoofing.

Alok Pandey et. al [4] have presented countermeasures for the MAC spoofing such as the MAC Address should be fetched directly from NIC instead of from the operating system [5].

rather it should have compared with the MAC Address from NIC. If it doesn't match it should delete the entry from OS or from registry.

The MAC addresses may be freezed by the router that introduces this for the supporting MAC filtering [6] and IP Reservation.

The MAC Address contained in the arriving ARP packets should not be checked against the MAC Address stored / recorded in the Operating System,

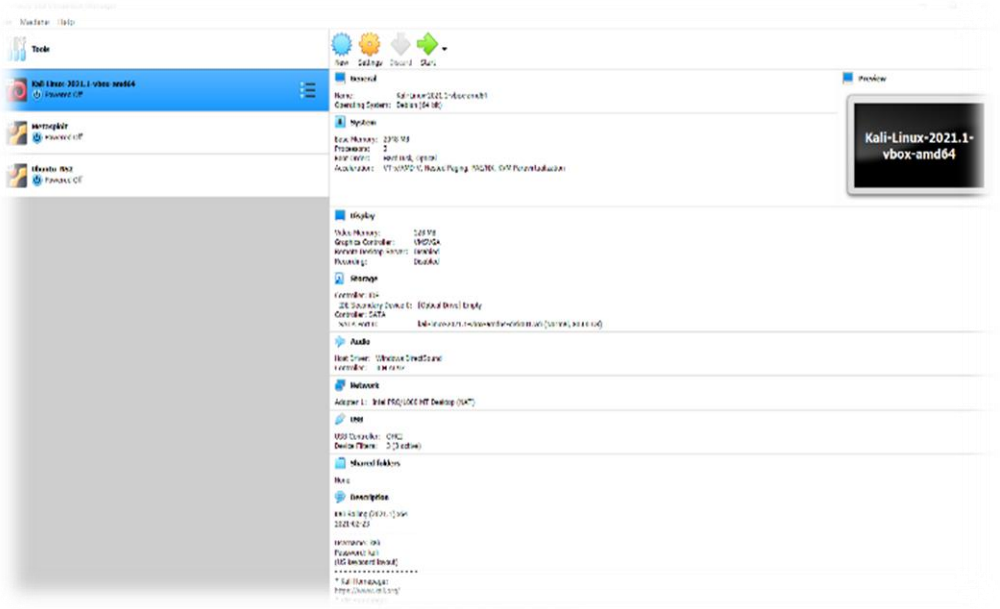


Fig.3Virtual Box window

Countermeasures and prevention procedure against MAC Spoofing.

The MAC addresses may be freezed by the router that introduces this for the supporting MAC filtering [6] and IP Reservation.

An Encryption is an alternative for the communication between the wireless PC and access point to prevent MAC spoofing.

Attack Environment

MAC spoofing is commits using set of steps. To demonstrate MAC Spoofing, an attack environment is created. To do this following steps and requirements are performed.

Step-1: Download and install oracle virtual box to configure attacker machine i.e. KALI LINUX.

Step-2: Download and install KALI LINUX operating system on virtual box.

Step-3: Open virtual box and start KALI LINUX.

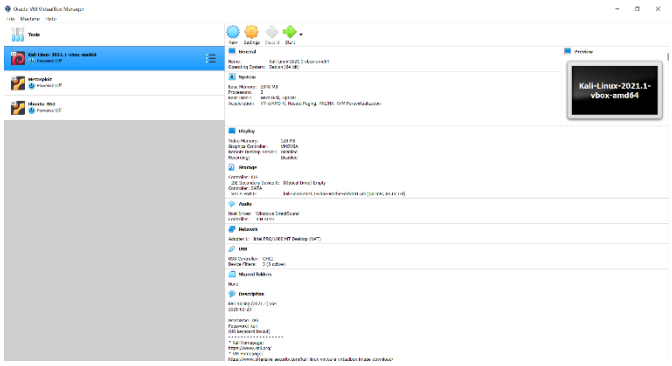


Fig.3Virtual Box window

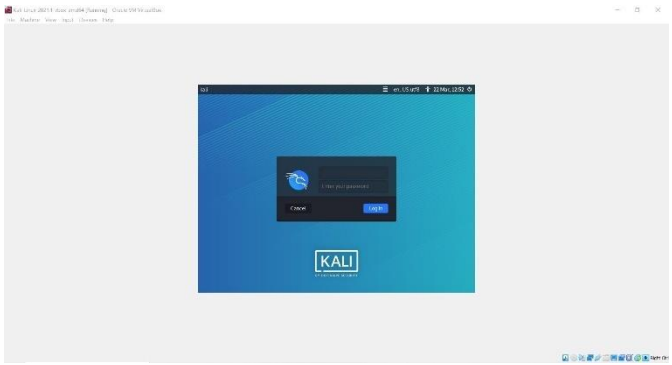


Fig.4KALI LINUX

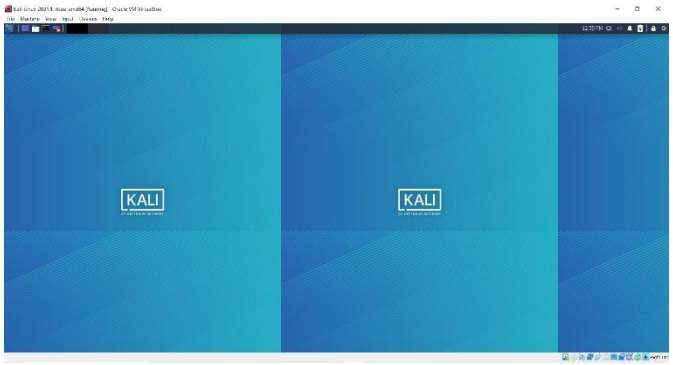


Fig.5kali Linux Desktop

Step-4: Once KALI LINUX has started, then open terminal.

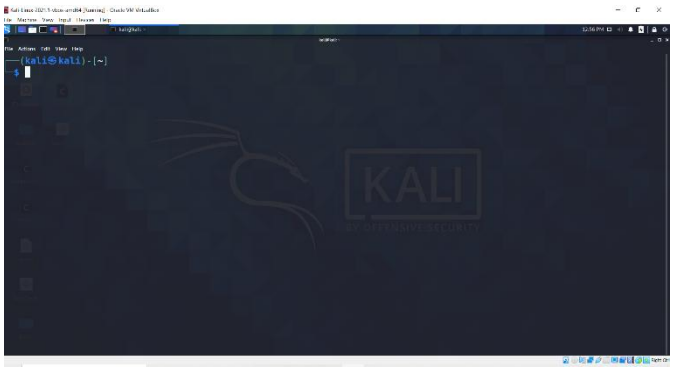


Fig.6Terminal Window

Step-5: Now, attack environment is ready. After this, attacker search target MAC address using network scanning or see its MAC address using ifconfig commands.

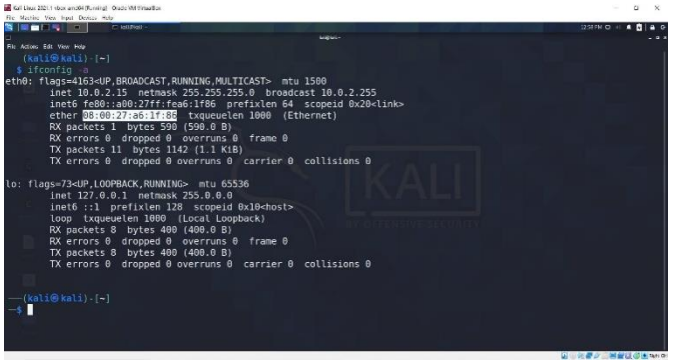


Fig.7Terminal Window

Step-6: When MAC address are found then use MACCHANGER command to change host MAC address to new address.

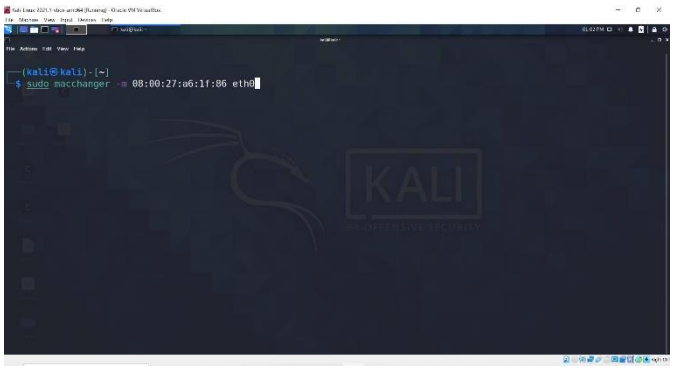


Fig.8MACCHANGER Command

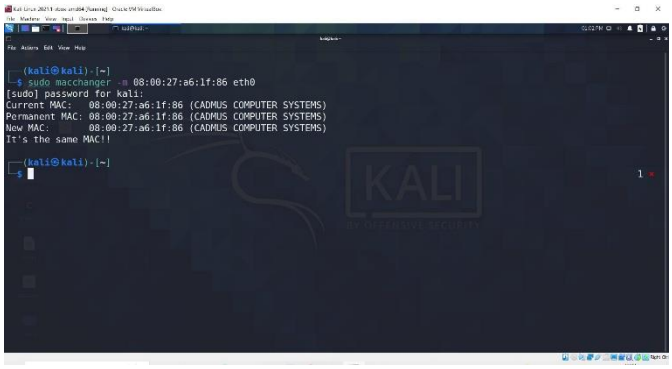
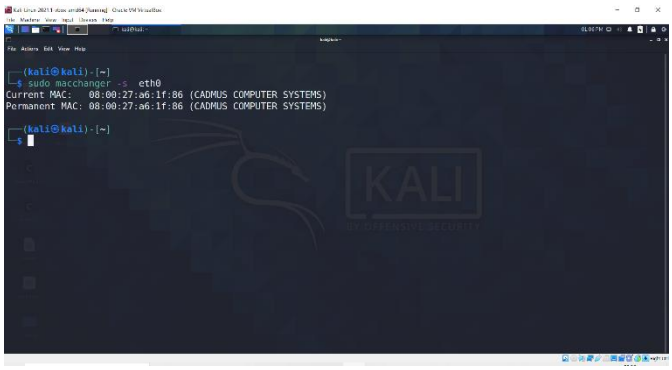


Fig.9macchanger Command



Conclusion:

Now-days, network users are continuously increases. With the same rate network attackers are also growing. Network and their resources are vulnerable to exploit by different kind of attacks such IP spoofing, MAC spoofing, E-mail spoofing, ping death etc. Here, MAC spoofing attack is studied. With this, implementation of MAC spoofing in KALI LINUX operating system also demonstrated.

References:

[1] Tanenbaum, “Computer Networks” -PHI Learning

[2] Forouzan, “TCP/IP-Protocol suite”, TMH 3rd edition

[3]David C. Plummer, “An Ethernet Address Resolution Protocol”, RFC-826, Network Working Group, November 1982.

[4] Alok Pandey, Dr. Jatinderkumar R. SainiCounter Measures to Combat Misuses of MAC Address Spoofing Techniques, Int. J. Advanced Networking and Applications 1358 Volume: 03, Issue: 05, Pages: 1358-1361 (2012).

[5] Min-kyu Choi, Rosslin John Robles, Changhwa Hong, Tai-hoon Kim, “Wireless Network Security: Vulnerabilities, Threats and Countermeasures”, International Journal of Multimedia and Ubiquitous Engineering, 3(3), July 2008, 516-520

[6] Arbaugh, William A., Shankar, Narendar, and Wan, Y.C. Justin, “Your 802.11 Wireless Networks have no clothes”, 2001