

R V COLLEGE OF ENGINEERING

Name: Dhanush M USN: 1RV18IS011 Dept/Lab: ISE/CSDF Expt No.: 04 a
Date: 06/12/2021 Title: SNIFFING AND SPOOFING TOOLS

a. MACCHANGER SPOOFING TOOL

INTRODUCTION

A media access control address is a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

It is a unique and hard coded address programmed into network devices which cannot be changed permanently. The MAC address is in the 2nd OSI layer and should be seen as the physical address of your interface.

Basically it's a hardware id used when connecting to Ethernet and Wi-fi.

As we know that MAC addresses are unique, that means every device has a MAC address that doesn't match with any other devices. We can't change it permanently, but we are able to spoof it. MACchanger will help us to do that.

Spoofing is to pretend to be someone else. It is a technique for temporarily changing your Media Access Control (MAC) address on a network device. Macchanger is a tool that is included with any version of Kali Linux including the 2016 rolling edition and can change the MAC address to any desired address until the next reboot.

For the normal purpose we don't need to change our MAC but in penetration testing this has many benefits.

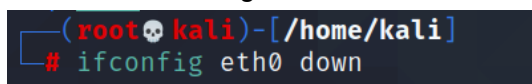
- Suppose some wireless system has blocked someone's original MAC address then it can be bypassed it easily, or
- One can spoof their original MAC address before performing penetration test activity on wireless networks so that the admin of the network can't see or ban the original MAC address. This means the admin can see or block/ban the spoofed MAC address.

Objectives - To perform spoofing.

EXECUTION STEPS

1. Can be accessed from the Terminal window in the Kali Linux system or MACchanger from Sniffing and Spoofing tools in the Start menu.
2. Before we get started, we need to take down the network adapter in order to change the MAC address. **To turn off network interface,**

Command - `ifconfig eth0 down`



```
(root@kali)~[/home/kali]
# ifconfig eth0 down
```

3. **Basic structure**

Syntax - `macchanger [options]`

a. **To show summary of options (-h --help)**

Command - *macchanger --help*

```
(root@kali)~# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help                Print this help
-V, --version             Print version and exit
-s, --show                Print the MAC address and exit
-e, --ending              Don't change the vendor bytes
-a, --another             Set random vendor MAC of the same kind
-A, --any                 Set random vendor MAC of any kind
-p, --permanent          Reset to original, permanent hardware MAC
-r, --random              Set fully random MAC
-l, --list[=keyword]      Print known vendors
-b, --bia                 Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX
  --mac XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
```

b. **To change MAC address (-m --mac)**

Syntax - *macchanger -m <new_MAC_address> eth0*

```
(root@kali)~# macchanger -m b2:aa:0e:56:ed:f7 eth0
Current MAC: 08:00:27:ab:08:1c (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:ab:08:1c (CADMUS COMPUTER SYSTEMS)
New MAC: b2:aa:0e:56:ed:f7 (unknown)
```

c. **To set a fully random MAC address (-r --random)**

Command - *macchanger -r eth0*

```
(root@kali)~# macchanger -r eth0
Current MAC: b2:aa:0e:56:ed:f7 (unknown)
Permanent MAC: 08:00:27:ab:08:1c (CADMUS COMPUTER SYSTEMS)
New MAC: 32:c4:fc:ed:dc:8a (unknown)
```

d. **To not change the vendor bytes (-e --ending)**

Command - *macchanger -e eth0*

```
(root@kali)~# macchanger -e eth0
Current MAC: 32:c4:fc:ed:dc:8a (unknown)
Permanent MAC: 08:00:27:ab:08:1c (CADMUS COMPUTER SYSTEMS)
New MAC: 30:c4:fc:33:6c:5c (unknown)

(root@kali)~# macchanger -e eth0
Current MAC: 30:c4:fc:33:6c:5c (unknown)
Permanent MAC: 08:00:27:ab:08:1c (CADMUS COMPUTER SYSTEMS)
New MAC: 30:c4:fc:25:43:75 (unknown)
```

- e. To reset MAC address to its original, permanent hardware value
(-p --permanent)

Command - `macchanger -p eth0`

```
(root@kali)-[/home/kali]
# macchanger -p eth0
Current MAC: 30:c4:fc:25:43:75 (unknown)
Permanent MAC: 08:00:27:ab:08:1c (CADMUS COMPUTER SYSTEMS)
New MAC: 08:00:27:ab:08:1c (CADMUS COMPUTER SYSTEMS)
```

4. To bring up the network interface

Command - `ifconfig eth0 up`

```
(root@kali)-[/home/kali]
# ifconfig eth0 up
```

CONCLUSION

1. The Macchanger is a simple tool which is easy to use and provides effective ways of spoofing Mac addresses.
2. Macchanger provides a way to conduct penetration testing without the owner knowing the permanent Mac address of the user.

REFERENCES

1. How to change MAC address using MACchanger on Kali Linux -
<https://linuxconfig.org/how-to-change-mac-address-using-macchanger-on-kali-linux>
2. MAC address spoofing with MACchanger in Kali Linux -
<https://www.hackingtutorials.org/general-tutorials/mac-address-spoofing-with-macchanger/>
3. MACchanger Tool -
<https://medium.com/%40arnavtripathy98/macchanger-tool-using-kali-linux-656817f73f30>
4. How to change/spoof your MAC address using MACchanger on Kali Linux -
<https://pentesttools.net/how-to-change-spoof-your-mac-address-using-macchanger-on-kali-linux-2018-1/>