**ZP Enterprises**

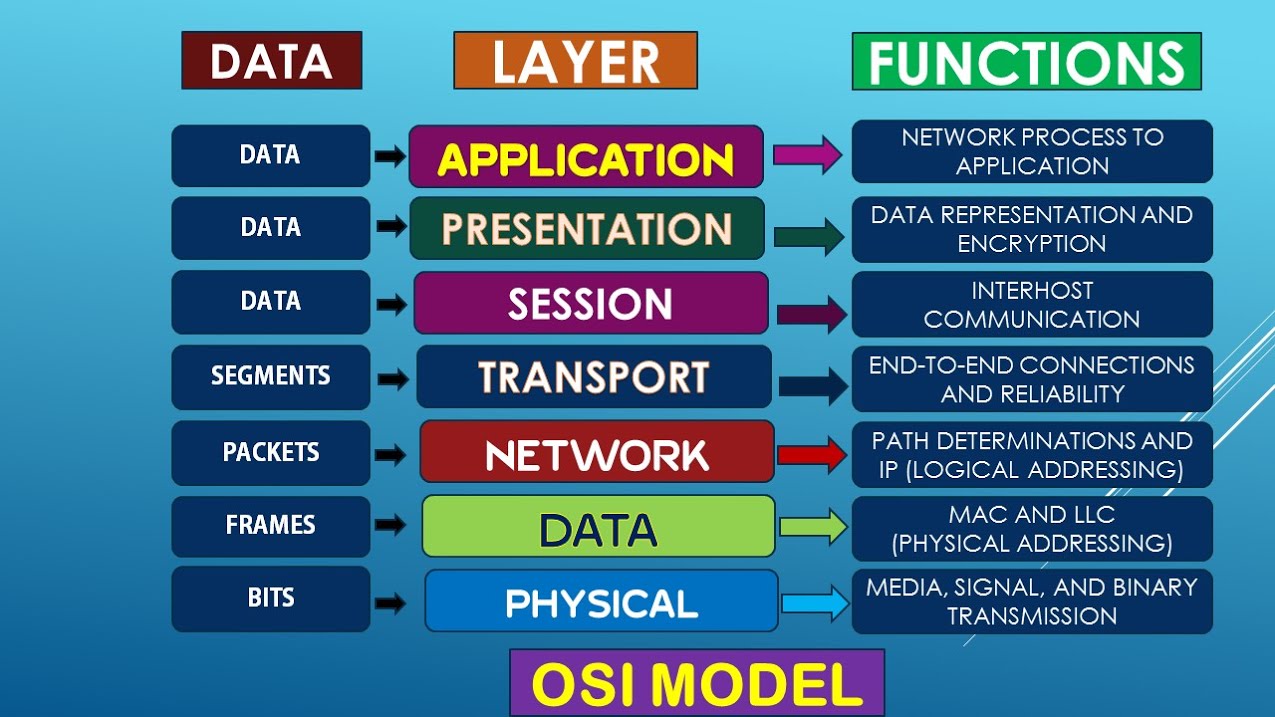
**How to Change the Mac Address in Kali Linux Using Macchanger?**

|  |  |
| --- | --- |
| Prepared By: | Zachary Pelka |
| Document Version: | 1.0 |
| Last Updated On: | 30SEP2020 |
| Document Classification: | Public Knowledge |

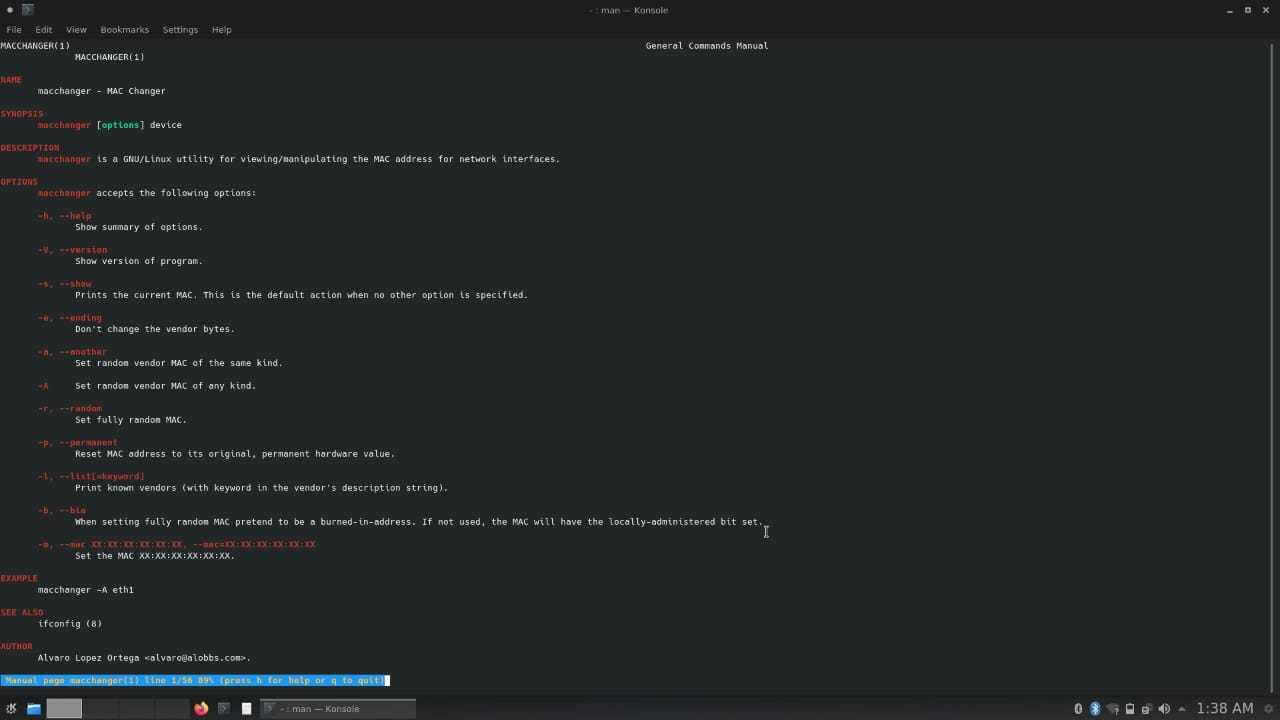
The information in the document may contain proprietary and confidential information that is intended for the employees of ZP Enterprises only. If you are not an employee of ZP Enterprises, you are hereby notified that any disclosure, copying, distribution, retention or use of the contents of this information is prohibited.

1. MAC Address
   1. MAC Address Technology Overview

Definition: The MAC address (short for media access control address) is the worldwide unique hardware address of a single network adapter. The physical address is used to identify a device in computer networks. This is the DATA layer as long as you have connectivity at the Physical Layer, and you should be thinking about this before any Red Team operations. Remedial training is needed if you do not know this and you should not be reading this document.



* 1. ****Change random mac address:****First, let us change the network card’s hardware MAC address to a random address. First, we will find the MAC address of the eth0 network interface (or whatever is appropriate for your configuration). To do this we execute macchanger with an option -s and an argument eth0.



We start and we execute macchanger with an option -s and an argument eth0.

macchanger -s eth0

Now the network interface you are about to change a MAC address should be turned off before changing the mac address. Use [ifconfig command](https://www.geeksforgeeks.org/ifconfig-command-in-linux-with-examples/) to turn off your network interface

ifconfig eth0 down

Now we can change the MAC address of the hardware by using the command

macchanger -r eth0

Once you have executed the command you can finally turn your network interface up

ifconfig eth0 down

Now you can display your MAC by using:

macchanger -s eth0

****Change specific MAC address:****

You can use MAC changer to change MAC of your choice follow the commands

ifconfig eth0 down

macchanger -m 00:d0:70:00:20:69 eth0

ifconfig eth0 up

macchanger -s eth0

Follow the same sequence as we did for random change, the only difference is that this time you have your specific MAC address with you. Use -l option to find a MAC address prefix of a specific hardware vendor:

macchanger -l

Set crontabs for rebooting  
  
  
crontab -e  
  
At the end of opened file, add these two lines (ETHERNET CARD : eth0 ; WIFI CARD : wlan0)  
  
  
@reboot macchanger -r eth0  
@reboot macchanger -r wlan0  
  
Save and close using (CTRL+o & CTRL+x)  
Now open /etc/NetworkManager/NetworkManager.conf  
  
  
nano /etc/NetworkManager/NetworkManager.conf  
  
If there is a connection section, leave first line and add next two lines  
  
  
[connection]  
ethernet.cloned-mac-address=preserve  
wifi.cloned-mac-address=preserve  
  
And now reboot the system and you can see the MAC address is changed  
Remember that this only works during reboot it will not work when you are logged in  
if you want changes to occur during the session is running, use this script  
You can also run the commands(Italic commands) in the terminal directly without the first line if you don't want to create the script:  
  
  
touch macc.sh  
nano macc.s  
  
Add these lines to the file  
  
  
#!/bin/bash  
service network-manager stop  
ifconfig eth0 down  
macchanger -r eth0  
ifconfig eth0 up  
ifconfig wlan0 down  
macchanger -r wlan0  
ifconfig wlan0 up  
service network-manager start  
  
Save and close nano  
Run these in terminal  
  
  
chmod +x macc.sh  
./macc.sh  
  
Voila! you just changed mac address during session

DISCLAIMER:

Do not attempt to do this at home, not knowing what you are doing or attempting to do harm to other systems. This document is for educational purposes only, and ZP Enterprises does not condone this.

We wish to point out that if a user spoofs the mac using either the terminal window or the method outlined in this thread, then goes to surf the net thinking the mac is spoofed, network manager overrides the spoofed mac address and uses its own setting found in the /etc/NetworkManager/system-connections/ folder. If there is no mac spoof address listed in the network-manager drop down menu and/or the system-connections folder then Network-manager uses the device mac. These mac spoofing routines run at start only hold true IF Network-manager is not called into play.  
  
We suggest users manually put in mac spoof addresses for all connection listed in network-manager.

If your network manager applet is not showing then type  
  
service network-manager start  
  
or  
  
service network-manager restart  
  
In a terminal window - either will work and start network-manager for you.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **By** | **Changes** |
| **1.0** | 02OCT2020 | Z. Pelka | Initial Document |
| **1.1** | ? | Z. Pelka | TBD |