Setup the fake access point using TP-Link TLWN772N in linux:

Step : 1

sudo apt update

sudo apt upgrade –y

sudo apt dist-upgrade –y

sudo apt autoremove

reboot

sudo apt install dkms

sudo -i echo "blacklist r8188eu" > "/etc/modprobe.d/realtek.conf"

exit

git clone https://github.com/aircrack-ng/rtl8188eus cd rtl8188eus

sudo ./dkms-install.sh

sudo apt autoremove

sudo

reboot

/\* To enable Monitor Mode

ifconfig

wlan0 down

airmon-ng check kill

iwconfig

wlan0 mode monitor

ifconfig

wlan0 up iwconfig

/\* To check Packet Injection \*/

aireplay-ng --test wlan0

To enable DHCP

dhcp

nano dnsmasq.conf

interface=wlan0mon

dhcp-range=192.168.1.2, 192.168.1.30, 255.255.255.0, 12h

dhcp-option=3, 192.168.1.1

dhcp-option=6, 192.168.1.1

server=8.8.8.8

log-queries

log-dhcp

listen-address=127.0.0.1

assign interface to network gateway

ifconfig wlan0mon up 192.168.1.1 netmask 255.255.255.0

route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1

start dns server

dnsmasq -C dnsmasq.conf -d

provide internet

iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

iptables --append FORWARD --in-interface wlan0mon -j ACCEPT

sudo bash –c ‘echo 1 > /proc/sys/net/ipv4/ip\_forward’

echo 1 | sudo tee /proc/sys/net/ipv4/ip\_forward