Setting up a SoftAP/FakeAP in Kali linux

Notebook:	3g		
Created:	5/18/2018 2:30 PM	**Updated:**	5/18/2018 2:43 PM
URL:	https://moneebazhar.wordpress.com/2015/11/15/setting-up-a-softapfakeap-in-kali-linux-2/		

Modified from: https://moneebazhar.wordpress.com/2015/11/15/setting-up-a-softapfakeap-in-kali-linux-2/

Kali linux makes setting up a soft access point a breeze. However, there are a couple of ways this can be done and you could end up trying to follow different tutorials and mixing it all up. In our case, we would be using the following tools.

- dnsmasq for a DHCP server.
- hostapd for creating the AP itself.
- dnschef (optional) if a custom DNS server is required. This will be discussed in a later tutorial or you can check out its documentation, it is pretty straightforward.

These tools come pre-installed in kali linux. You can confirm by running the following command in terminal:

> *sudo apt-get install dnsmasq hostapd dnschef*

This tutorial assumes that you have a kali linux distro installed on a virtual machine (VM) or a physical machine. Prior programming experience is not required, a wireless card which supports packet injection and softAP is necessary. If you are on a VM, an external card is a must, the built in one won't do. Now, to the interesting part.

Putting your wireless card in monitor mode

The very first thing you need to do is put your wireless card in monitor mode and give it an IP address. More often than not, the name assigned to the wireless interface is 'wlan0'. Type the following in terminal:

> *sudo airmon-ng start wlan0*
> *sudo ifconfig wlan0mon 10.0.0.1/24*

Configuring dnsmasq

As mentioned earlier, dnsmasq will be used for our DHCP server. This, essentially, hands out IP addresses to all clients connected to our softAP. Other DHCP servers can also be used if you are comfortable with an alternative. In terminal, type:

> *sudo nano /etc/dnsmasq.conf*

This will open the dnsmasq configuration file. At the end of this file, enter the following information.

> *no-resolv*
> *no-poll*
> *interface=wlan0mon*
> *bind-interfaces*
> *dhcp-range=10.0.0.2,10.0.0.250,255.255.255.0,12h*
> *dhcp-option=1, 255.255.255.0*
> *dhcp-option=3, 10.0.0.1*
> *dhcp-option=6, 8.8.8.8*
> *dhcp-leasefile=/var/lib/misc/dnsmasq.leases*
> *log-queries*

Configuring hostapd

Getting hostapd to run can be a great deal of pain sometimes. It might throw errors at you the first, second, third or as many times as you run it. The best way is to go through its documentation at least once before getting started. Here is the link. Most probably you will find a solution to your specific problem in the documentation. You can also leave a comment here and I will try to help out as soon as possible. In my case the error was the infamous invalid/unknown driver 'nl80211'. I solved this by compiling hostapd from source. Once you are done setting up, open up your hostapd.conf file and enter the following at the end:

> *interface=wlan0mon*
> *driver=nl80211*
> *ssid=test # you can set as you wish*
> *channel=1*
> *hw_mode=g*
> *wpa=2*
> *wpa_passphrase=my-secret-password # you can set as you wish*
> *wpa_key_mgmt=WPA-PSK*

```
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
ctrl_interface=/var/run/hostapd
```

Last few steps

We are almost done. What we need now is to enable packet forwarding between our softAP and the actual physical interface which is connected to the internet. Run the following in terminal:

```
sudo iptables -t nat -F
sudo iptables -F
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -A FORWARD -i wlan0mon -o eth0 -j ACCEPT
sudo iptables -A FORWARD -i eth0 -s 208.54.0.0/16 -j DROP      # T-
mobile
sudo iptables -A FORWARD -i eth0 -s 68.31..0.0/16 -j DROP      # Sprint
sudo iptables -A FORWARD -i eth0 -s 141.207.0.0/16 - j DROP    # Verizon
sudo iptables -A FORWARD -i eth0 -s 129.192.0/16 - j DROP     # AT&T
sudo echo '1' > /proc/sys/net/ipv4/ip_forward
```

You can check using by iptables -L

You are all set. Finally you need to fire up dnsmasq and hostapd.

```
sudo /etc/init.d/dnsmasq stop
sudo /etc/init.d/dnsmasq start
cd *path to your hostapd directory*
sudo ./hostapd hostapd.conf
```

Hopefully everything went correctly and your softAP will appear in the list of wireless APs like other APs. You can test it out by connecting your cellphone or a second PC/laptop to it. If you do not get it in the first try, don't sweat it. Leave a comment with your problem and we will find a solution :).