Wardriving With Tyler

Hello everyone, these are my steps for wardriving. Hopefully you can try this **legal** and fun activity with me!

Step 1: Buy a USB wireless adapter

The only reason this is step 1 is because you will have to purchase this in advance. So please plan ahead if you plan to do this with EHC.

The most important thing you can do is to find a network adapter that works with Linux.

Please double-triple check that it does so as this is obviously the most important thing. Don't be like me and buy the cheapest one and it not work. The below URL is a link to the USB wifi adapter I purchased. It comes with instructions on how to install the drivers and worked perfectly. You can definitely find another, but this one works well. I honestly couldn't find one cheaper than $20, but you might can. It's a risk but can pay off if you want to save money.

https://www.amazon.com/dp/B07FCNP2VL?psc=1&ref=ppx_yo2ov_dt_b_product_details

Step 2: Install a Virtualization Software and VM

To wardrive you will need a linux machine. From what I can find a Debian based machine will work best, but you are welcome to try another type of virtual machine. First, install your virtualization software you plan to use. I used vmware pro (and you can get a free trial of 30 days if you'd like) But I am sure virtualbox or vmware workstation will work as well. M1 users, use whatever you can.

Download a Linux VM, it can be whatever you prefer. I recommend using Kali Linux, it actually comes preinstalled with the tool we will be using later. But install a linux vm (preferably Debian based). Then import it to your virtualization software and get it to run.

Step 3: Install drivers

Install the necessary drivers on your linux machine for the adapter to work. If you will be using my USB adapter. The instructions can be found here.
https://linux.brostrend.com/

It does say that sometimes it works out of the box, but I honestly didn't even check. It says it does, but I went ahead and downloaded the drivers.

If not, there isn't much more I can say. Just be sure to search through your package for the instructions because it *should* come with some.

Step 4: Install Kismet(Not needed with Kali)

If you aren't using kali, you will have to install Kismet. Below are the docs on the kismet website. The will tell you how to install it

https://www.kismetwireless.net/docs/readme/installing/linux/

Step 5: Pass our vm the adapter usb

Go up into settings and click removable devices (in vmware) it should show a list of usb devices plugged in to your computer. You will want to connect the one that says Realtek 802.11ac NIC(if you use mine) to your vm. Click on it and say disconnect from host or connect to VM. It should show a dot next to it and will say disconnect from vm if you try to do it again. If you are using my network card you will see it flashing blue in the corner.

Step 6: Set network card to be in monitor mode

First you will want to run either 'ip a' or ifconfig. In this list you should see your network adapter listed, if not, your drivers aren't installed or isn't done properly. It will more than likely be named wlan0 or wlan1. Mine was wlan0. You will want to run the following command:

"Sudo airmon-ng start YourCardName"

You will want to replace YourCardName with either wlan0 or whatever it is called. This will put our card in monitor mode.

Step 6: Launch Kismet

Now all is left is kismet, you will want to launch kismet. In future cases, you will probably want to create a nonroot user that can run kismet. However, I don't care so I will use sudo. This is how you start kismet using your network adapter

"Sudo kismet -c YourCardName"

After this the terminal will output a ton of text: Like this

```
INFO: Detected new 802.11 Wi-Fi access point 78:D2:94:0B:45:CB
INFO: 802.11 Wi-Fi device 78:D2:94:0B:45:CB advertising SSID 'NETGEAR26-5G'
INFO: Detected new 802.11 Wi-Fi access point 94:A6:7E:C1:0E:F8
INFO: 802.11 Wi-Fi device 94:A6:7E:C1:0E:F8 advertising SSID 'NETGEAR18-5G'
INFO: Detected new 802.11 Wi-Fi access point 38:94:ED:A7:1C:0A
INFO: 802.11 Wi-Fi device 38:94:ED:A7:1C:0A advertising SSID 'High IQ
      Hotspot'
INFO: Detected new 802.11 Wi-Fi access point BC:A5:11:01:72:F9
INFO: 802.11 Wi-Fi device BC:A5:11:01:72:F9 advertising SSID 'NETGEAR68-5G'
INFO: Detected new 802.11 Wi-Fi access point A8:B1:3B:D2:57:29
INFO: 802.11 Wi-Fi device A8:B1:3B:D2:57:29 advertising SSID 'DIRECT-27-HP
      DeskJet 2700 series'
INFO: Detected new 802.11 Wi-Fi access point BC:A5:11:FC:83:FE
INFO: 802.11 Wi-Fi device BC:A5:11:FC:83:FE advertising SSID 'NETGEAR50-5G'
INFO: Detected new 802.11 Wi-Fi access point F0:81:75:0B:11:7F
INFO: 802.11 Wi-Fi device F0:81:75:0B:11:7F advertising SSID
      'MySpectrumWiFi78-5G'
INFO: Detected new 802.11 Wi-Fi access point 06:19:5D:6E:03:15
INFO: 802.11 Wi-Fi device 06:19:5D:6E:03:15 advertising SSID 'Spectrum
      Mobile'
```

If you see this text, Congrats! You are now successfully wardriving! Next you can click at the top where it says to point your browser and open that interface. It will open a gui on a browser that will be pleasant to look at.

From here on out, you can now war drive!

If you are doing this for the EHC competition, make sure to save it to an output file for logging purposes!

Happy Hunting!

Reference:

https://null-byte.wonderhowto.com/how-to/use-kismet-watch-wi-fi-user-activity-through-walls-0182214/