Windows利用WSL2+USB外置网卡实现实时wifi sniffer抓包

wlan接入 wlan射频 **朱恺** 2024-01-19 发表

组网及说明

类linux系统比如kali-linux与macos等都具备成熟可靠的wifi sniffer方式，配合wireshark可以做到简单的操作就能完成实时wifi sniffer抓包。

但是在windows下一直没有可靠稳定的方式去实现这个功能。综合起来大概有这么几种：

1、 付费软件实现：omnipeek、AirPCAP（软件及配套网卡——已停产），缺点是正版付费价格昂贵，非吾等兴趣玩家首选。

2、 Wireshark下的Npcap方式实现抓包，缺点：操作繁琐且存在BUG →*在Windows电脑上通过wireshark直接无线抓包的方式 - 知了社区 (h3c.com)*

3、 Windows出品的microsoft network monitor软件（已不更新），目前笔者暂未搞定如何调整wifi网卡做sniffer捕获无线报文，只能实现自己笔记本的wifi报文抓取。

所以一直困扰使用windows电脑作为工作主力工具的我。如果各位也有希望windows下能够实现wifi报文即时sniffer分析的需求，可以接下来耐心阅读。以下内容我前前后后遇到了各种坑，研究了近2周时间。谨以此文，给各位读者一些思路和指导，以及少走弯路。

告警信息

核心思路：

Windows下开启WSL2（精简的虚拟机运行linux系统），安装kali-linux系统，使用kali下的aircrack-ng工具来对wifi网卡设置成monitor模式（wifi sniffer的关键）。

需要解决：

1、 如何把windows下的usb网卡挂载到kali-linux下。

2、 Usb网卡在kali-linux下的驱动文件。

3、 Wireshark读取到网卡并进行无线捕获，并且如同windows下的应用一样方便。

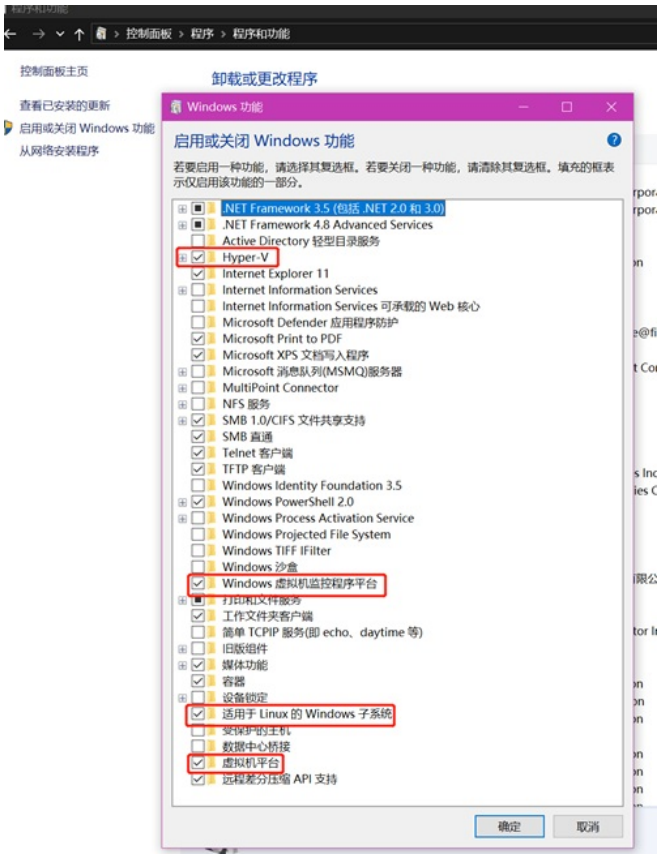
问题描述

准备工作：

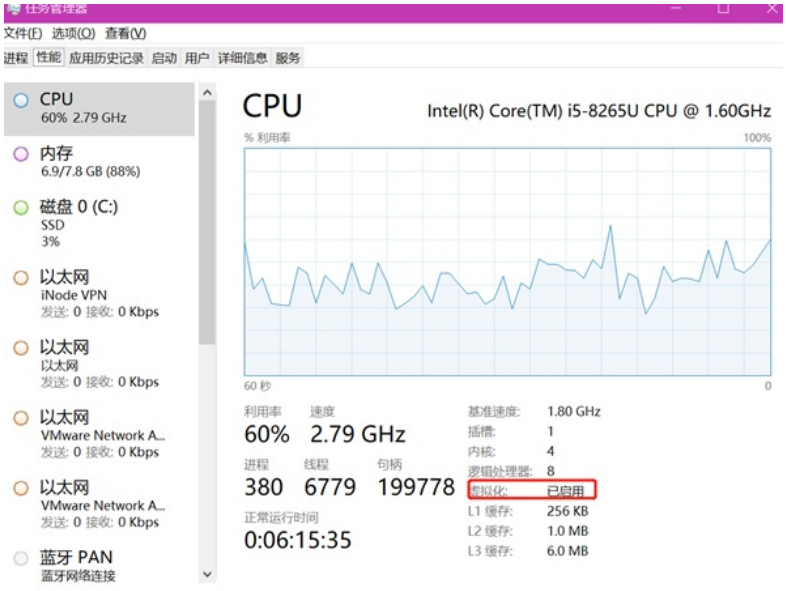
1、 windows PC 要求更新到最新版本，本例为win10企业版 22H2 内部版本号19045.3930。更新到最新版本！更新到最新版本！更新到最新版本！ 因为没有更新到最新版本，花费了我一周半的时间。Win10易升 更新工具：下载 Windows 10 (microsoft.com)

2、 usb网卡。本例为TPLINK 8812AU网卡，类似的逻辑usb外置的其他网卡应该也可以。

3、 windows PC找到控制面板的“程序”“启用或关闭windows功能”，勾选如下红框特性。完成后重启：



重启后检查PC的CPU是否有虚拟化特性：



过程分析

阶段1-安装WSL2。

参考资料：适用于 Linux 的 Windows 子系统文档 | Microsoft Learn

升级完windows10更新之后。可以在管理员模式下的打开powershell工具（按住win+X，可以找到入口）。在powershell下执行（推荐用windows terminal工具Windows 终端安装 | Microsoft Learn）

```
wsl --install
```

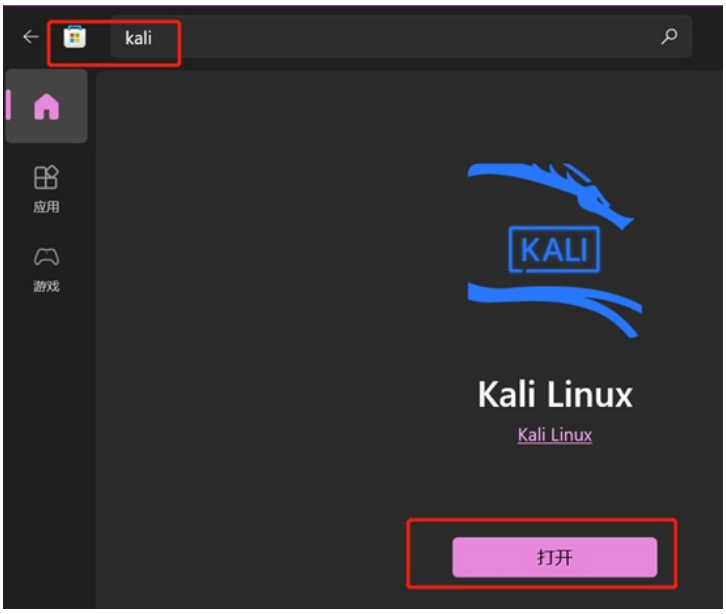
完成wsl的基础功能安装之后执行,更新检查适用于此windows版本的linux widnows子系统

```
wsl --update
```

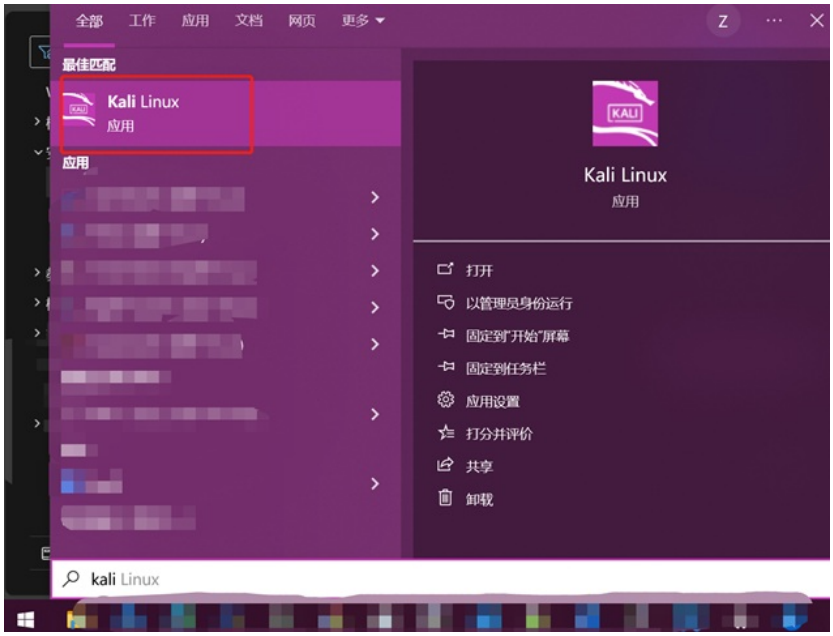
并通过设置默认的WSL模式版本为2，WSL历史上存在过version1和2.目前使用2较为常见。

```
wsl --set-default-version 2
```

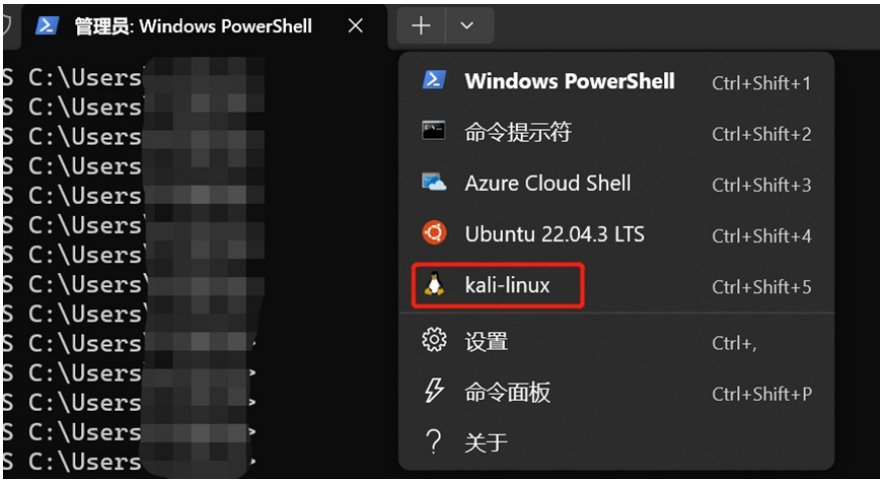
然后打开windows的Microsoft store去下载linux发行版本，比如本例下载kali-linux

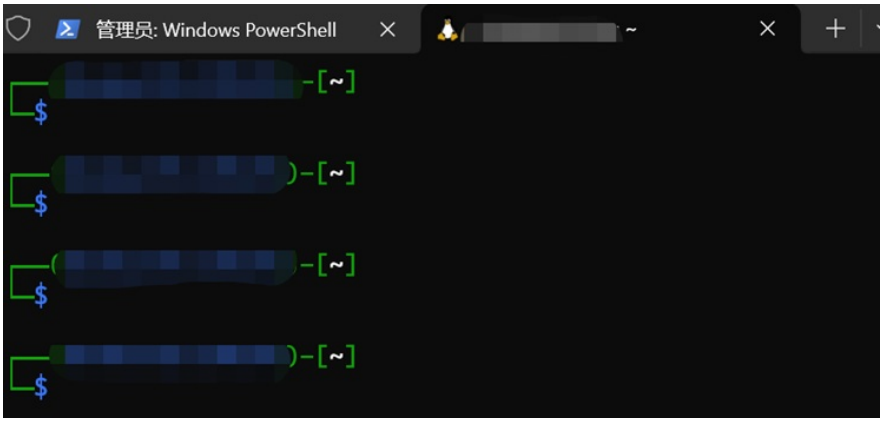


完成下载之后会在windows的开始菜单找到kali-linux的入口



点击后可以进入kali-linux的bash交互界面，也可以在windows terminal自然找到入口进入，第一次登陆会要求输入账号密码，比例以wireless为例：wireless/wireless





至此简单的WSL2+kali-linux就已经安装完毕。接下来要准备对USB网卡进行挂载操作。

阶段2 挂载USB网卡

这里用到windows下的usbipd工具，可以实现把windows外界的usb设备挂载到WSL2下。当然了挂载到kali-linux下就会在window上消失这个usb设备。参考文档：连接 USB 设备 | Microsoft Learn

Powershell下执行

```
winget install --interactive --exact dorssel.usbipd-win
```

在kali-linux的bash下执行

```
sudo apt install linux-tools-generic hwdata
sudo update-alternatives --install /usr/local/bin/usbip usbip /usr/lib/linux-tools/*-generic/usbip 20
```

通过必要的重启电脑之后，再次运行powershell下的命令：

```
usbipd.exe list
```

就可以看到当前挂载在windows系统下的usb设备，例如：

```
PS C:\Users\      > usbipd.exe list
Connected:
BUSID  VID:PID    DEVICE                                                  STATE
1-2    1b3f:2008  USB Audio Device, USB 输入设备                          Not shared
1-10   8087:0aaa  英特尔(R) 无线 Bluetooth(R)                              Not shared
4-4    2357:0101  TP-Link Wireless USB Adapter                            Shared
```

通过命令：

```
usbipd.exe bind -b 4-4
```

实现USB网卡的shared，只有shared才可以被attach给wsl系统。

在你的例子中4-4需要被换成其他实际值

```
PS C:\Users\      > usbipd.exe bind -b 4-4
usbipd: warning: Unknown USB filter 'hdlpdbk' may be incompatible with this software; 'bind --force' may be required.
usbipd: warning: USB filter 'USBPcap' is known to be incompatible with this software; 'bind --force' will be required.
```

再通过命令attach给wsl系统

```
usbipd.exe attach -w kali-linux -b 4-4
```

```
PS C:\Users\      > usbipd.exe attach -w kali-linux -b 4-4
usbipd: info: Selecting a specific distribution is no longer required. Please file an issue if you believe that the default selection
 mechanism is not working for you.
usbipd: info: Using WSL distribution 'kali-linux' to attach; the device will be available in all WSL 2 distributions.
usbipd: info: Using IP address 172.17.192.1 to reach the host.
usbipd: warning: A third-party firewall may be blocking the connection; ensure TCP port 3240 is allowed.
```

如果你不知道自己wsl的名称 通过wsl -l -v来获取即可

```
PS C:\Users\      > wsl -l -v
  NAME                   STATE           VERSION
* Ubuntu-22.04           Stopped         2
  docker-desktop-data    Stopped         2
  kali-linux             Running         2
```

然后你会发现原本windows下的usb网卡不见了，取而代之在kali-linux下通过lsusb可以发现存在usb网卡

```
lsusb
```

```
┌──(      )-[~]
└─$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 2357:0101 TP-Link RTL8812AU Archer T4U 802.11ac
Bus 001 Device 004: ID 2357:0101 TP-Link RTL8812AU Archer T4U 802.11ac
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
```

到此是不是感觉都很顺利很正常？呵呵，接下来才是难受的。

在kali下执行ifconfig并没有发现这个usb网卡被识别，那么应该是kali没有这个网卡驱动导致的。

好的，这就去弄支持aircrack的RTL8812AU网卡驱动，结果发现还需要kali环境下做编译驱动。

在尝试编译驱动时又发现因为WSL属于特殊定制的linux发行版，缺少了linux kernel header，没办法进行驱动编译。

此时需要更新内核文件重新编译新的kernel文件加载，并且确保header存放路径正确。一整个大写的 服!

阶段3 更新kali-linux kernel及header

这里参考文档kevin-doolaeghe/wsl-kernel-modules: Build kernel modules for WSL2 distros (github.com)

按照指导的操作步骤来一般不会出错。

一、wsl2 kali的基础设置

1、 更新系统文件

```
sudo apt update && sudo apt upgrade -y
```

2、 安装必要的组件

```
sudo apt install bash-completion build-essential gcc g++ avr-libc avrdude default-jre default-jdk git clang make nano xz-utils usbip wget
source .bashrc
```

3、 安装kali linux文件

```
sudo apt install kali-linux-large
```

4、 开启远程接入，桌面GUI等

```
sudo apt install kali-win-kex
```

二、build并且安装自定义的WSL2 linux kernel内核

1、安装必要的工具

```
sudo apt install flex bison libssl-dev libelf-dev git dwarves bc
```

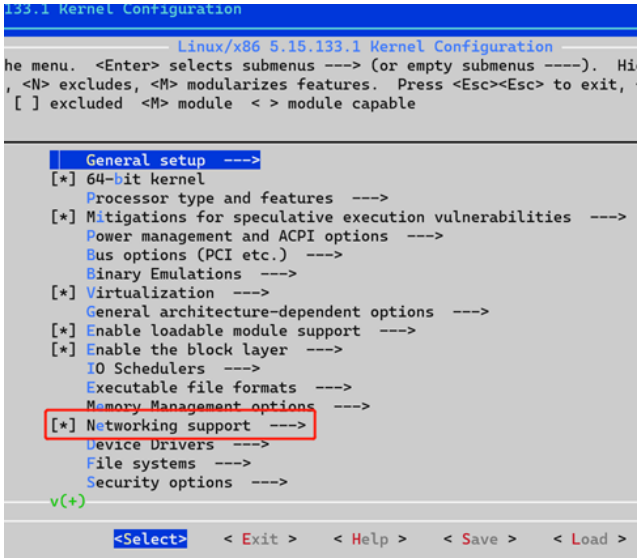
2、下载官方的WSL2内核文件并且做安装前的准备

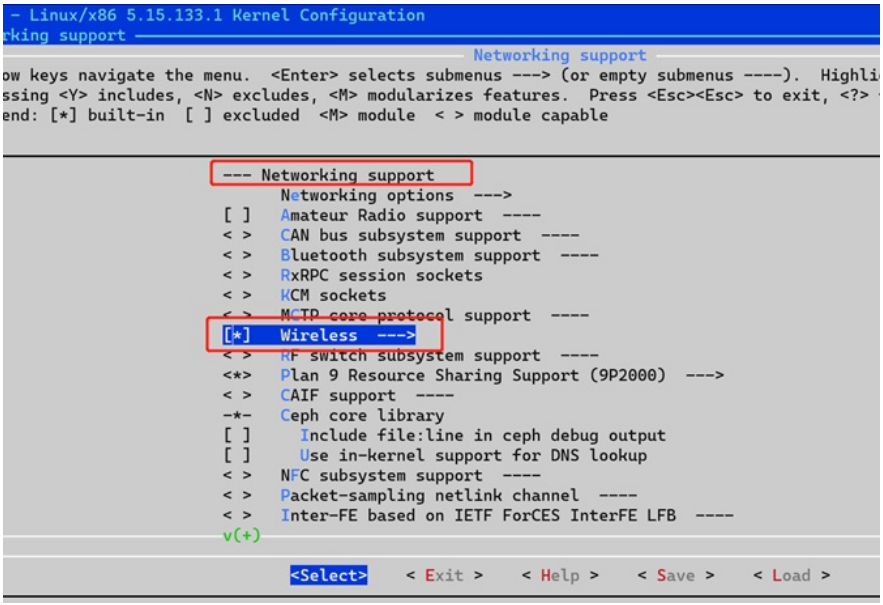
```
wget https://github.com/microsoft/WSL2-Linux-Kernel/archive/refs/tags/linux-msft-wsl-$(uname -r | cut -d- -f 1).tar.gz
tar -xvf linux-msft-wsl-$(uname -r | cut -d- -f 1).tar.gz
cd WSL2-Linux-Kernel-linux-msft-wsl-$(uname -r | cut -d- -f 1)
cat /proc/config.gz | gunzip > .config
make prepare modules_prepare -j $(expr $(nproc) - 1)
```

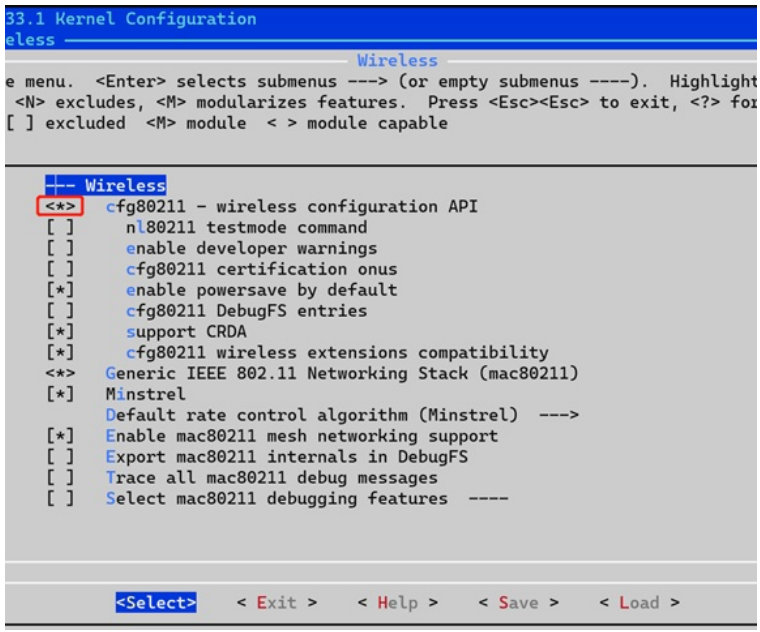
3、打开内核的配置菜单，选择network下的wireless cfg80211相关的内容

```
make menuconfig -j $(expr $(nproc) - 1)
```

按上下选择，按Y确认，按回车进入下级菜单，最后保存退出，部分截图：







4、 build内核并且安装

make modules -j $(expr $(nproc) - 1)

sudo make modules_install

make -j $(expr $(nproc) - 1)

sudo make install

这个过程中可能会遇到报错：

arch/x86/Makefile:142: CONFIG_X86_X32 enabled but no binutils support

我的解决办法是

sudo vi ~/WSL2-Linux-Kernel-linux-msft-wsl-$(uname -r | cut -d- -f 1)/arch/x86/Makefile

然后找到142行，与CONFIG_X86_X32相关的整段注释掉。重新执行

Sudo make install

5、 make install结束后会在当前目录下产生一个vmlinux文件，我们需要放到windows下的用户目录，执行：

cp vmlinux /mnt/c/Users/wireless/

6、 在windows下的用户目录创建.wslconfig并且指定内核文件位置。

nano /mnt/c/Users/wireless/.wslconfig

文件内填写

[wsl2]

kernel=C:\\Users\\wireless\\vmlinux

7、 在windows powershell下关闭重启wsl

wsl –shutdown

然后重新在powershell拉起kali-linux

阶段4 编译网卡驱动并且装载驱动识别RTL8812AU

1、 下载aircrack-ng关于rtl8812au的网卡驱动包，其他网卡自行研究

git clone https://github.com/aircrack-ng/rtl8812au

cd rtl8812au

2、 编译驱动

sudo make

3、 编译成功后会得到.ko文件，我们尝试测试下驱动文件

sudo modprobe cfg80211

sudo insmod 88XXau.ko

lsmod

4、 安装驱动

sudo mkdir -p /lib/modules/$(uname -r)/kernel/drivers/net/wireless

sudo make install

5、 启用此module

sudo modprobe 88XXau

6、 在系统启动时自动加载，因为wsl会频繁伴随windows的开关机 //这里可能还有点小问题，如果发现驱动没有加载重新执行下**sudo modprobe 88XXau**

echo "cfg80211" | sudo tee -a /etc/modules-load.d/cfg80211.conf

echo "88XXau" | sudo tee -a /etc/modules-load.d/88XXau.conf

阶段5 kali安装aircrack-ng及wireshark工具调用wifi网卡

1、 安装airchrack-ng工具

sudo apt install aircrack-ng pciutils

2、把网卡设置成monitor模式

sudo airmon-ng start wlan0//我的例子是wlan1，通过ip a来检查是哪个网卡编号

```
┌(                    )-[~/WSL2-Linux-Kernel-linux-msft-wsl-5.15.133.1]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group defau
    link/ether 00:15:5d:cb:14:e4 brd ff:ff:ff:ff:ff:ff
    inet 172.17.201.157/20 brd 172.17.207.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fecb:14e4/64 scope link
       valid_lft forever preferred_lft forever
5: wlan1: <BROADCAST,MULTICAST> mtu 2312 qdisc noop state DOWN group default qlen
    link/ether 88:25:93:b0:66:9d brd ff:ff:ff:ff:ff:ff

┌(                    )-[~/WSL2-Linux-Kernel-linux-msft-wsl-5.15.133.1]
└─$ sudo airmon-ng start wlan1

PHY     Interface       Driver          Chipset

phy2    wlan1           88XXau          TP-Link RTL8812AU Archer T4U 802.11ac
                (monitor mode enabled)
```

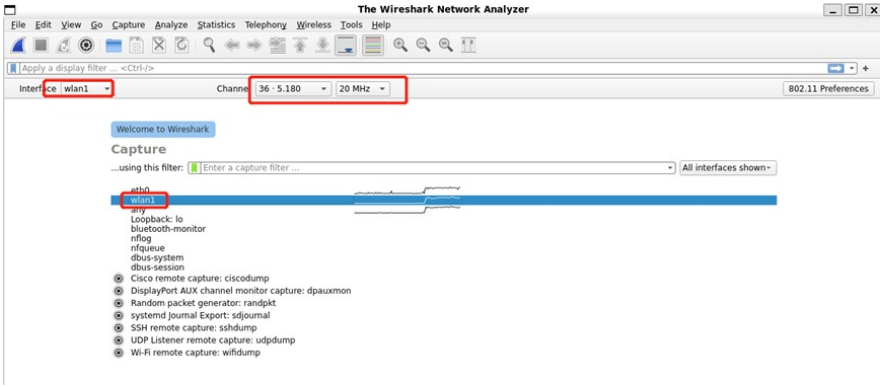
3、安装wireshark

sudo apt install wireshark

4、 用root模式运行wireshark，如果不是root会发现识别不了这个网卡

sudo wireshark

弹出的wireshark窗口就能显示wlan1这个网卡，通过点击view下的wireless bar你甚至可以从容的在抓包前选择工作信道，如下图：



然后have fun

本教程结束。

解决方法

最后的思考：

这个案例在整理之前本人遇到过很多问题，但是都逐渐找到网上的资料能够解决应对，几度推倒重做甚至想要放弃，但是最后还是坚持下来实现了。有人问为什么要折腾这个，有什么意义吗？能对实际工作学习带来多大的帮助吗？其实很多东西不一定在当下就一定是有价值的，但是如果不去突破不去思考可能永远不会迈出去前进的那一步，即使看起来那一步没有什么意义，但是谁知道呢？说不定这一步是未来成为高手的第一步。

再次感谢互联网上各种参考的资料。在整个整理的过程有很多其他参考的资料没有写明出处，但是都曾或多或少指导过我。我们始终是站在巨人肩膀上前进的。