PRÁCTICA 1-1. Configuración de un laboratorio virtual con Kali y comandos en ciberseguridad (I).

- Instalar y vincular al kernel un chipset WiFi compatible. Para ilustrar el proceso y comandos empleados vamos a instalar y asociar el driver del chipset Realtek RTL8812BU que puede descargarse desde el sitio de Github: https://github.com/cilynx/rtl88x2bu.git... Driver: rtl88x2bu-5.8.7.1_35809.20191129_COEX20191120-7777

- ☐ Generalmente en estos recursos indican si hay nuevos drivers actualizados y cómo descargarlos e instalarlos. En este caso vamos a elegir una máquina con PARROT OS sobre VMWARE (o en su caso el VIRTUALBOX). El proceso es idéntico para cualquier distribución DEBIAN como el KALI o el MINT. Los pasos son los siguientes:

  (1) Una vez arrancada la máquina insertamos el adaptador WiFi y seleccionamos conectarse a LINUX además de comprobar que es reconocida en el entorno de virtualización dependiendo si es VIRTUALBOX o VMWARE el proceso debería ser automático si es un chipset reciente y compatible...

```
┌──[vicky@parrot]─[~]
└──╼ $sudo git clone https://github.com/ivanovborislav/rtl88x2bu
[sudo] password for vicky:
Clonando en 'rtl88x2bu'...
remote: Enumerating objects: 951, done.
remote: Counting objects: 100% (259/259), done.
remote: Compressing objects: 100% (208/208), done.
remote: Total 951 (delta 115), reused 151 (delta 50), pack-reused 692
Recibiendo objetos: 100% (951/951), 4.41 MiB | 4.15 MiB/s, listo.
Resolviendo deltas: 100% (401/401), listo.
┌──[vicky@parrot]─[~]
└──╼ $
```

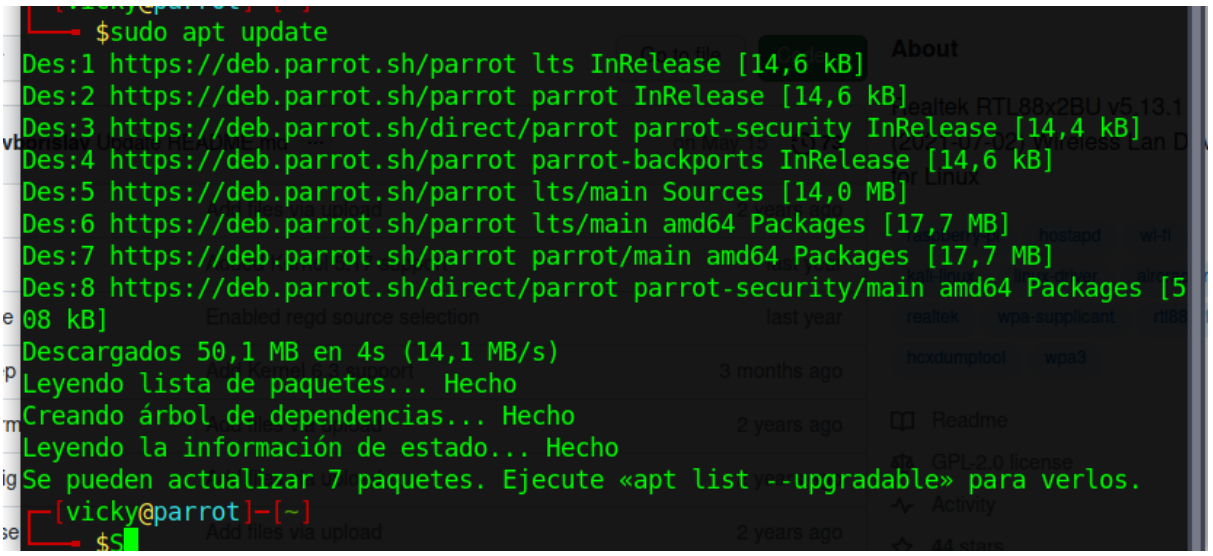
☐ Generalmente en estos recursos indican si hay nuevos drivers actualizados y cómo descargarlos e instalarlos. En este caso vamos a elegir una máquina con PARROT OS sobre VMWARE (o en su caso el VIRTUALBOX). El proceso es idéntico para cualquier distribución DEBIAN como el KALI o el MINT. Los pasos son los siguientes:

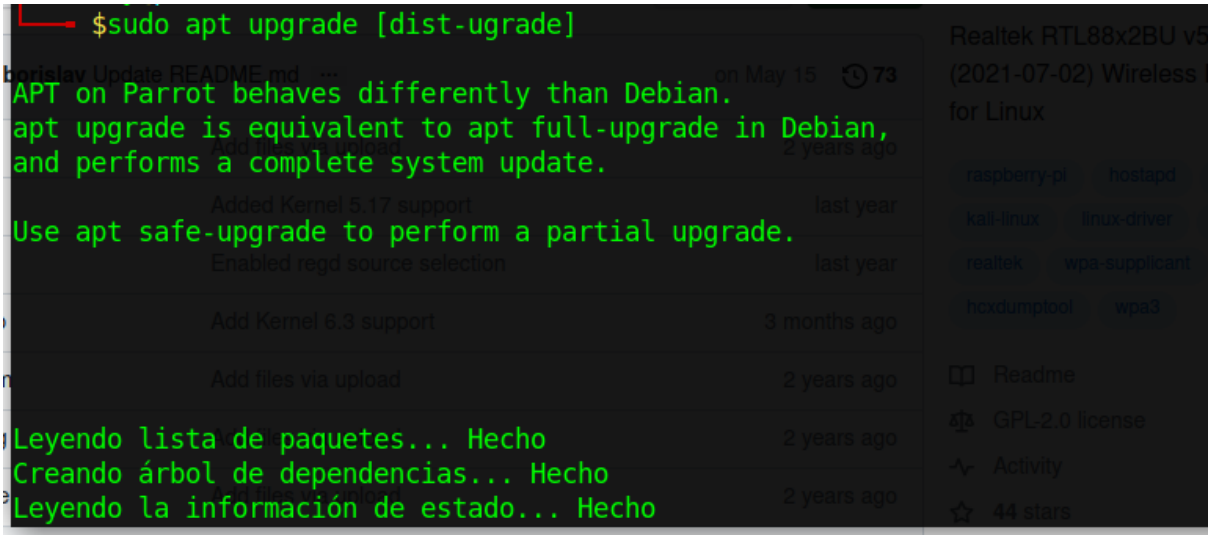
(1) Una vez arrancada la máquina insertamos el adaptador WiFi y seleccionamos conectarse a LINUX además de comprobar que es reconocida en el entorno de virtualización dependiendo si es VIRTUALBOX o VMWARE el proceso debería ser automático si es un chipset reciente y compatible...

(2) Identificamos el chipset y localizamos el driver más actualizado que en este caso es el rtl88x2bu-5.8.7.1. Pero antes de empezar, se debe realizar una actualización del sistema. El significado de la palabra "upgrade" es "actualizar" o "mejorar" y cuando utilizamos dicha opción, estaremos actualizando los paquetes del sistema a una versión superior, aunque no todos los paquetes serán actualizados. Paquetes "críticos", como aquellos relacionados con el KERNEL LINUX quedarán fuera de dicho upgrade. Si lo que queremos es solamente actualizar los programas "habituales" de nuestro equipo GNU/LINUX DEBIAN antes de hacer el UPGRADE, es recomendado hacer un "update" previo.

dist-upgrade | full-upgrade: actualiza las aplicaciones, herramientas y utilidades e instala el nuevo núcleo del Kernel Linux del sistema operativo. También elimina los paquetes antiguos si es necesario para la actualización. Es la opción más usada a la hora de actualizar un sistema por completo a una versión superior. Antes de hacer el DIST-UPGRADE, es recomendado hacer un "UPDATE" previo. Después hacer "FULL-UPGRADE" y reiniciar REBOOT.

- ✓ sudo apt update
- ✓ sudo apt upgrade [dist-upgrade]
- ✓ sudo apt full-upgrade





(3) Instalar las dependencias KMS y los PAQUETES EL GIT con los comandos:

- ✓ sudo apt install dkms git
- ✓ sudo apt install dkms git bc

```
┌─[vicky@parrot]─[~]
└──╼ $sudo apt install dkms git
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
dkms ya está en su versión más reciente (3.0.3-4parrot1).
fijado dkms como instalado manualmente.
git ya está en su versión más reciente (1:2.39.2-1~bpo11+1).
El paquete indicado a continuación se instaló de forma automática y ya no es nec
esario.
  libopengl0
Utilice «sudo apt autoremove» para eliminarlo.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

(4) Instalamos las dependencias del driver desde: git clone https://github.com/cilynx/rtl88x2BU o la alternativa, https://github.com/RinCat/RTL88x2BU-Linux-Driver.git ... a continuación pasamos al directorio del paquete con: cd rtl88x2BU o bien cd RTL88x2BU-Linux-Driver... y hecho esto, vamos a cargar en una variable provisional 'VER' la versión del fichero, para no tener que repetirla:

VER=$(sed -n 's/\PACKAGE_VERSION="\(.*\)"/\1/p' dkms.conf)

```
┌─[✗]─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $VER=$(sed -n 's/\PACKAGE_VERSION="\(.*\)"/\1/p' dkms.conf)
┌─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $
```

(5) Pasamos el driver al directorio con su versión donde se instalarán los paquetes y ordenamos la instalación. De esta forma, el comando se adapta a cualquier versión y no hay que estar copiándola para evitar errores:

sudo rsync -rvhP ./ /usr/src/rtl88x2bu-${VER}

```
└──╼ $sudo rsync -rvhP ./ /usr/src/rtl88x2bu-$(VER)
bash: VER: orden no encontrada
sending incremental file list
created directory /usr/src/rtl88x2bu-
./
Kconfig
            110 100%    0,00kB/s    0:00:00 (xfr#1, to-chk=761/763)
License
         18,43K 100%   17,58MB/s    0:00:00 (xfr#2, to-chk=760/763)
Makefile
         75,51K 100%   72,01MB/s    0:00:00 (xfr#3, to-chk=759/763)
README.md
         11,54K 100%   11,00MB/s    0:00:00 (xfr#4, to-chk=758/763)
clean
             64 100%   62,50kB/s    0:00:00 (xfr#5, to-chk=757/763)
dkms.conf
            257 100%  250,98kB/s    0:00:00 (xfr#6, to-chk=756/763)
halmac.mk
```

(6) Enlazar y asociar con el kernel (ver versión con uname -r) e instalar cabeceras si hace falta: apt install linux-headers-$(uname -r)

```
┌─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $sudo apt install linux-headers-$(uname -r)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
linux-headers-6.1.0-1parrot1-amd64 ya está en su versión más reciente (6.1.15-1p
arrot1).
fijado linux-headers-6.1.0-1parrot1-amd64 como instalado manualmente.
El paquete indicado a continuación se instaló de forma automática y ya no es nec
esario.
  libopengl0
Utilice «sudo apt autoremove» para eliminarlo.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
┌─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $
```

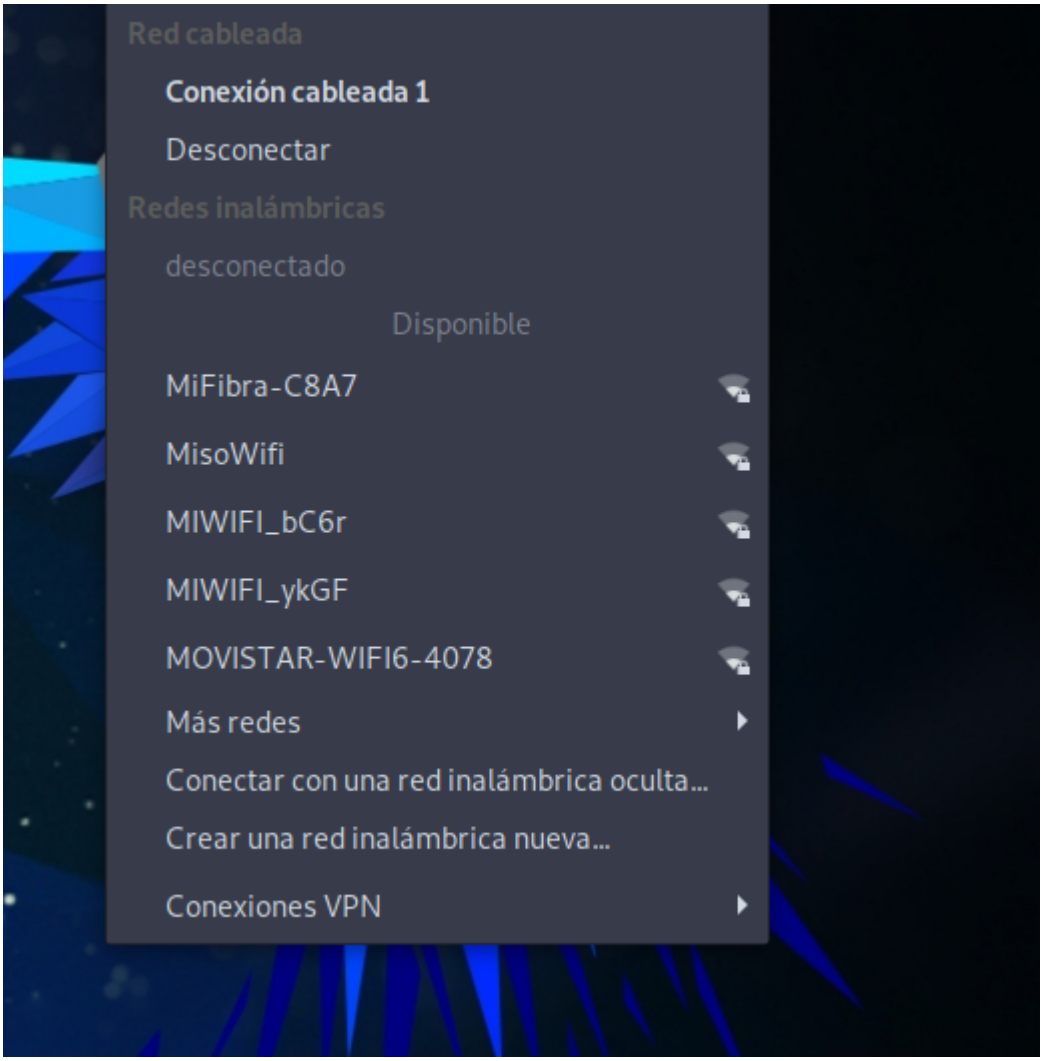
- ✓ sudo dkms add -m rtl88x2bu -v ${VER}
- ✓ sudo dkms build -m rtl88x2bu -v ${VER}

```
└──╼ $sudo make
make ARCH=x86_64 CROSS_COMPILE= -C /lib/modules/6.1.0-1parrot1-amd64/build M=/ho
me/vicky/rtl88x2bu  modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.1.0-1parrot1-amd64'
  CC [M]  /home/vicky/rtl88x2bu/core/rtw_cmd.o
  CC [M]  /home/vicky/rtl88x2bu/core/rtw_security.o
  CC [M]  /home/vicky/rtl88x2bu/core/rtw_debug.o
  CC [M]  /home/vicky/rtl88x2bu/core/rtw_io.o
```

(7) Finalmente, llegamos al último proceso de instalación (no de configuración), donde instalamos el DRIVER y hacemos una llamada al módulo para su comprobación. La antena estará visible y detectará redes cercanas...

- ✓ sudo dkms install -m rtl88x2bu -v ${VER}
- ✓ sudo modprobe 88x2bu
- ✓ sudo modprobe 88x2bu rtw_switch_usb_mode=1 (alternativa).

```
┌─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $sudo make install
install -p -m 644 88x2bu.ko  /lib/modules/6.1.0-1parrot1-amd64/kernel/drivers/ne
t/wireless/
/sbin/depmod -a 6.1.0-1parrot1-amd64
┌─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $sudo modprobe 88x2bu
┌─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $
```



- **Realizar la configuración en modo monitor.** En un entorno inalámbrico, los datos se transfieren del dispositivo a Internet en forma de paquetes enviando una solicitud de paquete al router. El enrutador recupera el paquete solicitado de Internet, y una vez que obtiene la página web, envía la información de vuelta a su dispositivo en forma de paquetes, controlando así todo el tráfico que va a los dispositivos conectados.

- El modo Monitor (Monitor Mode) en KALI | PARROT, permite leer todos los paquetes de datos, incluso si no se envían a través de este modo, y controla el tráfico recibido en redes inalámbricas; siendo capaz de capturar todos estos paquetes, que no solo están dirigidos al dispositivo, sino también a otros dispositivos conectados a la red.

- Dentro del hacking ético, el modo monitor se utiliza para capturar todos los paquetes de datos relevantes para comprobar si el router o la red es vulnerable y también para observar grandes volúmenes de tráfico de red.

- Para habilitarse el modo de monitor WiFi existen varios métodos. Todos los métodos no funcionan para todos los adaptadores porque no todos los adaptadores admiten el modo de monitor WiFi y existe una lista de adaptadores WiFi que admiten el modo monitor en: https://kalitut.com/usb-wi-fi-adapters-supporting-monitor/

IMAGEN	NOMBRE	CARACTERÍSTICAS
	Alfa AWUS1900	• Chipset: Realtek RTL8814AU • Antenas: 4 antenas
	Alfa AWUS036ACH	• Chipset: Realtek RTL8812AU • Antenas: 2 antenas
	TRENDnet AC1900	• Chipset: Realtek RTL8814AU • Antenas: 4 antenas
	TP-Link TL-WN722N	• Chipset: Atheros AR9271 • Antenas: 1 antenas
	TP-Link AC1900 Archer T9UH	• Chipset: Realtek RTL8814AU • Antenas: 1 antenas
	Alfa AWUS036NHA	• Chipset: Atheros AR9721 • Antenas: 1 antenas

... El mejor adaptador WiFi depende del uso y el entorno de trabajo, no hay un "Mejor adaptador WiFi" porque a veces se necesita trabajar en silencio y necesitamos un adaptador pequeño de corto alcance WiFi, y a veces trabajamos en la "jungla" y necesitamos el dispositivo más potente y sensible con antenas grandes...

RTL8812AU y RTL8814AU

La diferencia entre los chipsets RTL8812AU y RTL8814AU en la capacidad de soportar un número diferente de antenas.

- RTL8812AU admite hasta 2 antenas,
- Realtek RTL8814AU admite hasta 4 antenas.

En algunos casos, dependiendo del diseño del circuito del fabricante del dispositivo o del firmware, una antena solo se puede utilizar para la transmisión, y la otra solo para la recepción. Además, algunos dispositivos funcionan solo en un rango de elección, otros en dos rangos simultáneamente. Esto también debe tenerse en cuenta al comprar dispositivos.

Algunos fabricantes, por ejemplo, Alfa AWUS036ACH, Alfa AWUS1900,TRENDnet TEW-809UB, utilizan chips adicionales (por ejemplo, amplificadores de señal) y pueden tener otras características agradables.

Para aquellos que deciden ahorrar dinero y comprar productos en sitios como AliExpress en los chipsets mencionados anteriormente. Las antenas pueden ser 2, 4 o incluso más, pero muy importante para estos chipsets de 2,4/5,0 GHz también es MIMO, que, cuando se usan múltiples antenas, aumenta la posibilidad de capturar un apretón de manos y también es crucial para lograr datos de velocidades de transmisión máximas bajo uso normal.

- ☐ Hay áreas donde hay abundancia de puntos de acceso de 5,0 GHz, pero en algunos lugares. Nuestras tareas son diferentes, nuestro entorno es diferente y el mejor adaptador wifi USB para KALI | PARROT LINUX también será diferente dispositivo. Por lo general, los adaptadores con antenas externas grandes suelen ser más sensibles y potentes (esto es importante).
- ☐ Aunque tanto el comando ifconfig como el comando iwconfig pueden funcionar, se consideran obsoletos y pueden no estar instalados en el sistema de forma predeterminada. Actualmente, para ver el nombre de la interfaz se emplea: sudo airmon-ng


```
┌──[x]─[vicky@parrot]─[~/rtl88x2bu]
└──╼ $iwconfig
lo        no wireless extensions.

enp0s3    no wireless extensions.

docker0   no wireless extensions.

wlxac15a2479f22  unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

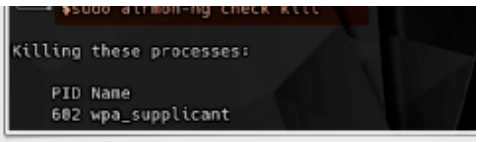
☐ Para localizar y cerrar cualquier proceso que pueda interferir con el uso del adaptador en MODO MONITOR, se pueden los siguientes comandos:

✓ sudo airmon-ng check
✓ sudo airmon-ng check kill

```
┌[vicky@parrot]-[~/rtl88x2bu]
└─ $sudo airmon-ng check

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    519 NetworkManager
    529 wpa_supplicant
```

```
┌[vicky@parrot]-[~/rtl88x2bu]
└─ $sudo airmon-ng check kill

Killing these processes:

    PID Name
    529 wpa_supplicant
```

☐ Localizado el nombre de la interfaz, se configura el modo monitor regresando a la carpeta de trabajo con cd rtl88x2BU y luego ejecutamos:



✓ sed -i 's/CONFIG_80211W = n/CONFIG_80211W = y/' Makefile
✓ sed -i 's/CONFIG_WIFI_MONITOR = n/CONFIG_WIFI_MONITOR = y/' Makefile

```
┌[✗]-[vicky@parrot]-[~/rtl88x2bu]
└─ $sudo sed -i 's/CONFIG_80211W=n/CONFIG_80211W =y/' Makefile
┌[vicky@parrot]-[~/rtl88x2bu]
└─ $
```

```
┌[vicky@parrot]-[~/rtl88x2bu]
└─$sudo sed -i 's/CONFIG_WIFI_MONITOR =n/CONFIG_WIFI_MONITOR y/' Makefile
┌[vicky@parrot]-[~/rtl88x2bu]
└─$
```

☐ Para habilitar el MODO MONITOR sin ninguna interferencia y desactivar el ADMINISTRADOR DE RED:
- ✓ sudo systemctl stop NetworkManager
- ✓ sudo airmon-ng start nombre_interfaz

```
┌[✗]-[vicky@parrot]-[~/rtl88x2bu]
└─$sudo airmon-ng start wlxac15a2479f22


PHY     Interface       Driver          Chipset

phy0    wlxac15a2479f22 rtl88x2bu       TP-Link Archer T3U [Realtek RTL8812BU]
                (monitor mode enabled)
```

☐ Para deshabilitar el modo Monitor, volver al administrador y reiniciar el administrador de red:

PHY
phy0

- ✓ sudo airmon-ng stop nombre_interfaz
- ✓ sudo systemctl start NetworkManager

☐ Realizar una prueba rápida de monitoreo del tráfico empleamos airodump-ng:

- ✓ sudo airodump-ng nombre_interfaz
- ✓ CTRL+C para salir.

```
┌[✗]-[vicky@parrot]-[~/rtl88x2bu]
└─$sudo airodump-ng wlxac15a2479f22
```

```
CH 10 ][ Elapsed: 0 s ][ 2023-08-09 11:39

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

0C:73:29:D8:1D:60  -83        0        0    0   9  130   WPA2 CCMP   PSK  sercommBA
28:9E:FC:45:2E:B6   16        9        6    2   6  195   WPA2 CCMP   PSK  <length:
94:91:7F:E6:85:DF  -42       10       12    3  11  130   WPA2 CCMP   PSK  MOVISTAR_

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   48:5F:99:A0:C0:D3   17    0 - 1     18        18
28:9E:FC:45:2E:B6  32:C1:AA:3B:AA:96  -78    0 - 1      0         2
```

- Configuración en modo monitor en KALI con la alternativa ifconfig | iwconfig. Se siguen los mismos (7) pasos vistos para Parrot anteriores salvo en la forma de configurar el modo monitor como alternativa a AIRMON-NG...

- Conocido el nombre de la interfaz, se regresa a la carpeta de trabajo con cd rtl88x2BU y luego ejecutamos:

  - ✓ sed -i 's/CONFIG_80211W = n/CONFIG_80211W = y/' Makefile
  - ✓ sed -i 's/CONFIG_WIFI_MONITOR = n/CONFIG_WIFI_MONITOR = y/' Makefile

- Aplicamos los comandos asignando nombre de interfaz:

  - ✓ make
  - ✓ sudo make install
  - ✓ sudo ifconfig nombre_interfaz down
  - ✓ sudo iwconfig nombre_interfaz mode monitor
  - ✓ sudo ifconfig nombre_interfaz up

```
┌──(root💀kali)-[/home/jxn/rtl88x2BU]
└─# sudo dkms install -m rtl88x2bu -v ${VER}

88x2bu.ko:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/5.14.0-kali4-amd64/kernel/drivers/net/

depmod.....

┌──(root💀kali)-[/home/jxn/rtl88x2BU]
└─# sudo modprobe 88x2bu
```

- Comprobamos con iwconfig tener el nombre de la interfaz en modo monitor y se realiza una prueba rápida de monitoreo del tráfico con airodump-ng. Con ella empezaremos a escuchar las WiFi y ver las MACs de los puntos de acceso, métodos de cifrado, velocidad, canales y los nombres que las redes inalámbricas que se escuchan por la antena.

```
┌──(root💀kali)-[/home/jxn/rtl88x2BU]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11b  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency:2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=-100 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

```
BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

14:2E:5E:86:FC:03   16       21        1    0   5  130   WPA2 CCMP   PSK  LowiFC02
66:29:ED:FD:85:1F  -68        2        0    0 108 1733   WPA2 CCMP   PSK  MOVISTAR_8511
78:29:ED:FD:85:1F  -68        2        0    0 108 1733   WPA2 CCMP   PSK  MOVISTAR_PLUS_8511
78:29:ED:FD:85:12  -73        3        0    0   1  130   WPA2 CCMP   PSK  MOVISTAR_8511
E0:51:63:93:1F:E1  -79        2        0    0 108 1733   WPA2 CCMP   PSK  <length:  0>
62:FD:DE:96:17:F5  -80        2        0    0 108 1733   WPA2 CCMP   PSK  <length: 10>
E6:B4:E6:99:50:6F  -81        2        0    0 108 1733   WPA2 CCMP   PSK  MOVISTAR_5061
FC:B4:E6:99:50:6F  -81        2        0    0 108 1733   WPA2 CCMP   PSK  MOVISTAR_PLUS_5061
EA:CA:12:D1:E2:84  -81        2        0    0  36 1733   WPA2 CCMP   PSK  MIWIFI_2G_XZym
62:FD:DE:96:17:F7  -82        2        0    0 108 1733   WPA2 CCMP   PSK  <length: 11>
5A:51:63:93:1F:E0  -82        2        0    0 108 1733   WPA2 CCMP   PSK  MiFibra-1FDE-5G
5A:51:63:93:1F:E2  -82        2        0    0 108 1733   WPA2 CCMP   PSK  MiFibra-1FDE
EA:CA:12:D1:E2:84  -82        2        0    0  36 1733   WPA2 CCMP   PSK  MIWIFI_5G_XZym
E0:51:63:93:1F:E0  -83        8        0    0   6  130   WPA2 CCMP   PSK  MiFibra-1FDE
78:DD:12:82:3D:C7  -84        2        0    0 108 1733   WPA2 CCMP   PSK  <length:  0>
E8:1B:69:95:FD:70  -86        9        0    0   6  130   WPA2 CCMP   PSK  vodafoneBA8860
6A:FD:DE:96:17:DA  -86        8        0    0  11  130   WPA2 CCMP   PSK  <length: 11>
Quitting...
```

... el mismo procedimiento debería desarrollarse en otros entornos de virtualización como VirtualBox aunque en la ejecución de monitoreo puede que se consuma mayor RAM.