Práctica #3: Comunicación Bluetooth

Curso: *Seguridad en Comunicaciones Inalámbricas*
Fecha de entrega:

Parte I
Cuestiones previas

1. inicia Kali Linux
2. Si va a usarlo en una máquina virtual, antes de iniciarlo configura el adaptador Bluetooth tal y como aparece en la imagen 1.

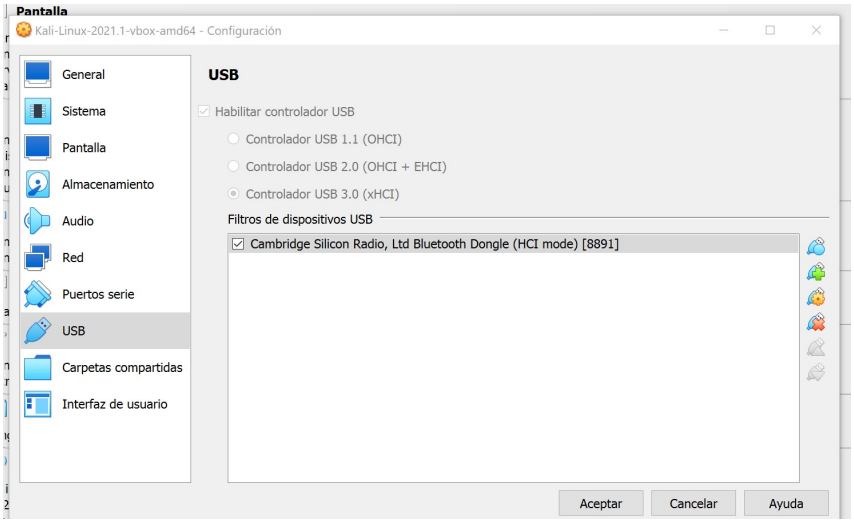

Figura 1: Configuración Dongle

Parte II
Soporte para Bluetooth en Kali

BlueZ es un conjunto de herramientas y bibliotecas de software de código abierto que implementa el protocolo Bluetooth en sistemas operativos basados en Linux. Esta suite de software permite la comunicación inalámbrica entre dispositivos, como auriculares, teclados, ratones, impresoras y una amplia variedad de dispositivos Bluetooth.

BlueZ es la implementación oficial de Bluetooth para el sistema operativo Linux. Proporciona soporte integral para dispositivos Bluetooth y permite la conexión, con-

figuración y comunicación entre ellos. Permite descubrir, emparejar y gestionar dispositivos Bluetooth desde la línea de comandos y mediante interfaces gráficas. Ofrece compatibilidad con Bluetooth Low Energy, lo que permite la conexión eficiente con dispositivos de baja potencia, como sensores y dispositivos de seguimiento. Incluye herramientas de línea de comandos como bluetoothctl que permiten interactuar con dispositivos Bluetooth, explorar perfiles GATT y realizar operaciones específicas.

Para más información consulta `https://documentation.ubuntu.com/core/explanation/system-snaps/bluetooth/#bluez`.

1. Comprueba si hay adaptador de Bluetooth activo: `$hciconfig`
   Salida:

   ```
   hci0:   Type: Primary  Bus: USB
   BD Address: XX:XX:XX:XX:XX:XX  ACL MTU: 310:10  SCO MTU: 64:8
   DOWN
   RX bytes:588 acl:0 sco:0 events:31 errors:0
   TX bytes:371 acl:0 sco:0 commands:31 errors:0
   ```

2. Si aparece DOWN, inicia la interfaz Bluetooth: `sudo hciconfig hci0 up`

3. Comprueba que la interfaz está activada: `$hciconfig`
   Salida:

   ```
   hci0:   Type: Primary  Bus: USB
   BD Address: XX:XX:XX:XX:XX:XX  ACL MTU: 310:10  SCO MTU: 64:8
   UP RUNNING
   RX bytes:1162 acl:0 sco:0 events:61 errors:0
   TX bytes:739 acl:0 sco:0 commands:61 errors:0
   ```

   Otra manera de comprobar si el servicio Bluetooth está funcionando:
   `systemctl status bluetooth.service`

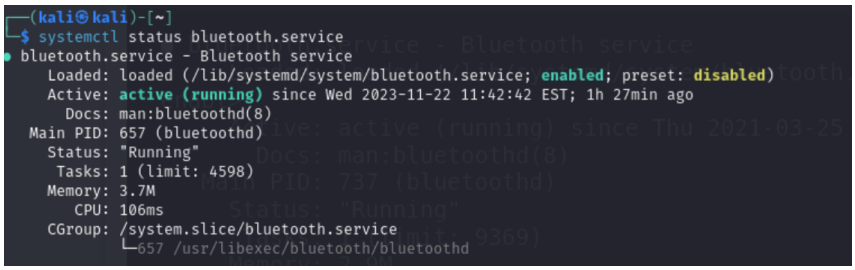

Figura 2:

4. En caso de no obtener respuesta al comprobar el adaptador Bluetooth (Paso1), ejecuta los siguientes comandos:

   a) instala el paquete BlueZ. `sudo apt-get install bluez`.

   b) `sudo systemctl enable bluetooth`

   c) `sudo systemctl start bluetooth`

5. Ejecuta los pasos 1,2 y 3.

1. Herramientas de Bluez: bluetoothctl

bluetoothctl (Bluetooth Control) es una herramienta interactiva con su propia línea de comandos.

Figura 3:

En caso de querer iniciar o apagar Bluetooth se pueden usar los comandos power on y power off. Tiene menús específicos para algunas tareas como para escanear.

1. Inicia `sudo bluetoothctl`.

   A continuación se detalla la secuencia recomendada para descubrir, listar y conectar dispositivos Bluetooth utilizando la herramienta `bluetoothctl` en sistemas Linux. Este procedimiento evita errores comunes (como la ausencia de dispositivos al ejecutar `devices` o fallos al conectar durante el escaneo).

   Dentro del intérprete de comandos ejecutar:

   ```
   power on
   agent on
   default-agent
   ```

   Estos comandos:

   - Encienden el adaptador Bluetooth.

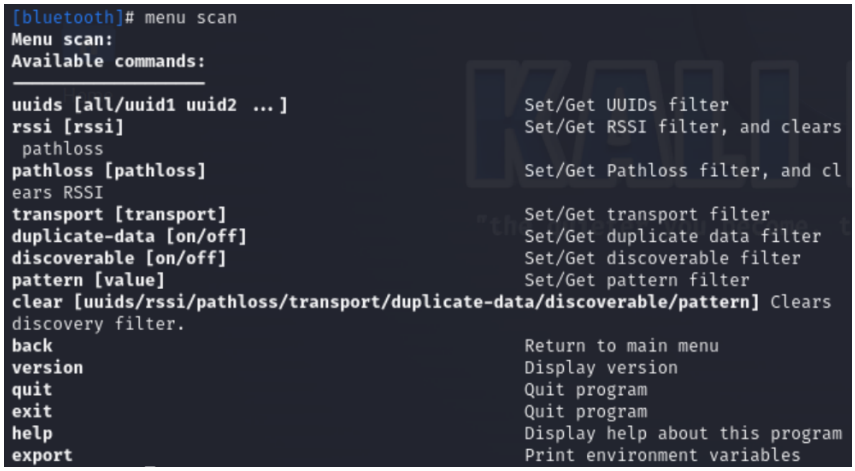

Figura 4:

- Activan el agente encargado de gestionar solicitudes del sistema.
- Registran un agente por defecto, necesario para almacenar y gestionar dispositivos.

2. Ejecutando `help` verás una serie de menús (en azul) y de comandos disponibles.
3. La primera actividad será escanear para encontrar los dispositivos cercanos: `scan on`. Para detectar sólo los dispositivos BLE puedes usar el comando `scan ble`

   Espere entre 10 y 15 segundos hasta observar mensajes del tipo:

   ```
   [NEW] Device XX:XX:XX:XX:XX:XX ...
   [CHG] Device ...
   ```

4. Detener el escaneo: Este paso es esencial. Mientras el escaneo está activo, `bluetoothctl` puede no registrar los dispositivos de manera consolidada.

   ```
   scan off
   ```

5. Lista los dispositivos cercanos con el comando `devices`
6. Escoge la dirección Bluetooth de uno de los dispositivos encontrados y solicita toda la información posible con el comando `info`. Este comando muestra información como:

   - Nombre y alias del dispositivo.
   - Estado de emparejamiento y conexión.
   - RSSI.
   - Lista de UUID y servicios soportados.

   En Bluetooth Low Energy (BLE) existen distintos tipos de direcciónes cuyo objetivo es equilibrar identificación, seguridad y privacidad. Algunas direcciónes son fijas y rastreables (como las públicas), mientras que otras se generan aleatoriamente para evitar el seguimiento del dispositivo por parte de terceros (como las RPA o las NRPA). La siguiente tabla resume sus diferencias principales:

Tipo	**Resoluble**	**Criptografia**	**Privacidad**
RPA (Resolvable Private Address)	Si (solo emparejados)	Si (IRK)	Muy alta
NRPA (Non-Resolvable Private Address)	No	No	Maxima privacidad, pero limita la funcionalidad
Static Random	No	No	Media
Public	Si (fija)	Si (MAC real)	Baja (rastreable)

   Según la *Bluetooth Core Specification*, el tipo de dirección Bluetooth se determina a partir de los dos bits más significativos (MSB) del primer byte de la dirección. Esto es, dado el primer byte `b7 b6 b5 b4 b3 b2 b1 b0`, los dos bits (b7 y b6) permiten clasificar la dirección en una de las siguientes categorías:

b7	b6	Tipo de dirección	Nombre
0	0	Public (IEEE MAC)	Public Device Address
1	1	Random Static	Static Random Address
0	1	Random Private (Non-Resolvable)	NRPA
1	0	Random Private (Resolvable)	RPA

Los dispositivos Bluetooth Clásico (BR/EDR) utilizan exclusivamente direcciónes **públicas**.

Indica de qué tipo son las direcciónes de los dispositivos detectados y comenta la información relevante.

7. Intenta conectarte a uno de los dispositivos encontrados indicando su dirección Bluetooth al comando `connect`. Antes de conectar, asegúrese de que el escaneo está detenido. ¿Qué información obtienes?

8. Entra en el menú gatt `menu gatt`. Para salir de un submenú ejecuta `back`.

9. Muestra los servicios disponibles en el dispositivo al que te has conectado: `list-attributes <dirección-bluetooth>`.

10. Selecciona uno de los servicios identificados usando su identificador uuid: `select-attribute <handle-del-servicio>`.

11. Muestra las características dentro del servicio seleccionado `characteristics`.

12. Selecciona una característica específica para obtener más detalles `select-attribute <handle-de-la-caracteristica>`

    Una vez que hayas seleccionado un servicio, puedes utilizar comandos como read, write o notify para interactuar con las características de ese servicio. Los detalles dependen del servicio y sus características.

    Por ejemplo, para leer una característica `read`, para escribir en una característica `write "00"` y para habilitar notificaciones para una característica `notify on`.

13. Para obtener información sobre la característica seleccionada, puedes usa el comando `info`.

14. Explorar los descriptores dentro de la característica seleccionada usando `char-desc`

15. Dada la traza siguiente comenta la información mostrada

```
[CHG] Device 63:D8:58:75:D9:F4 Connected: yes
Connection successful
[NEW] Primary Service (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service0006
00001801-0000-1000-8000-00805f9b34fb
Generic Attribute Profile
[NEW] Characteristic (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service0006/char0007
00002a05-0000-1000-8000-00805f9b34fb
Service Changed
```

```
[NEW] Descriptor (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service0006/char0007/desc0009
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
[NEW] Primary Service (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service000a
0000180a-0000-1000-8000-00805f9b34fb
Device Information
[NEW] Characteristic (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service000a/char000b
00002a29-0000-1000-8000-00805f9b34fb
Manufacturer Name String
[NEW] Characteristic (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service000a/char000d
00002a24-0000-1000-8000-00805f9b34fb
Model Number String
[NEW] Primary Service (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service000f
d0611e78-bbb4-4591-a5f8-487910ae4366
Vendor specific
[NEW] Characteristic (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service000f/char0010
8667556c-9a37-4c91-84ed-54ee27d90049
Vendor specific
[NEW] Descriptor (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service000f/char0010/desc0012
00002900-0000-1000-8000-00805f9b34fb
Characteristic Extended Properties
[NEW] Descriptor (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service000f/char0010/desc0013
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
[NEW] Primary Service (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service0014
9fa480e0-4967-4542-9390-d343dc5d04ae
Vendor specific
[NEW] Characteristic (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service0014/char0015
af0badb1-5b99-43cd-917a-a77bc549e3cc
Vendor specific
[NEW] Descriptor (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service0014/char0015/desc0017
00002900-0000-1000-8000-00805f9b34fb
Characteristic Extended Properties
[NEW] Descriptor (Handle 0x0000)
/org/bluez/hci0/dev_63_D8_58_75_D9_F4/service0014/char0015/desc0018
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
```

2. En caso de problemas

En caso de problemas instala de nuevo Blez e inicia el servicio. Ejecuta de uno en uno estos comandos y vete comprobando si la interfaz está activa:

```
sudo apt-get install bluez
sudo service bluetooth start
sudo service bluetooth restart
```

Parte III
Trabajando con Apps

- Instalación de nRF Connect y nRF Logger: Instala estas aplicaciones desde la tienda de aplicaciones de tu dispositivo móvil:
  - Android:
    - `https://play.google.com/store/apps/details?id=no.nordicsemi.android.mcp&hl=en&gl=US&pli=1`
    - `https://play.google.com/store/search?q=nrf+logger&c=apps&hl=en&gl=US`
  - iOS: `https://apps.apple.com/es/app/nrf-connect-for-mobile/id1054362403`[1]

Interpretacion de etiquetas en nRF Connect

Durante el escaneo de dispositivos BLE, la aplicacion *nRF Connect for Mobile* muestra diversas etiquetas e indicadores que ayudan a entender el tipo de dispositivo, su capacidad de conexión y su impacto en la seguridad y la privacidad. En la Tabla III se resumen las mas relevantes.

[1] No hay una versión de nRF Logger para iOS

Etiqueta	**Significado**
Find Me	Indica que el dispositivo implementa el perfil BLE *Find Me Profile*. Suele exponer el servicio `Immediate Alert (0x1802)` y la caracteristica `Alert Level (0x2A06)`, permitiendo localizar fisicamente el dispositivo (hacerlo sonar, vibrar, encender un LED, etc.).
Hand Off	Etiqueta utilizada por nRF Connect para indicar que el dispositivo anuncia datos propietarios relacionados con funciones de *handover* o cambio de rol/estado (por ejemplo, ciertos auriculares TWS que cambian entre auricular principal y secundario). No corresponde a un perfil BLE estandar, sino a logica especifica del fabricante.
Nearby	El dispositivo presenta un RSSI alto, lo que sugiere que se encuentra fisicamente muy cerca del smartphone. Es un buen candidato para realizar pruebas de conexión o captura de trafico.
Connectable	El dispositivo se encuentra en modo *connectable*, es decir, acepta conexiónes BLE (no es simplemente un beacon de solo anuncio).
Scannable	El dispositivo puede responder a *scan requests* con informacion adicional en el *scan response* (por ejemplo, nombre completo o datos extra), ademas del paquete de advertising inicial.
Non-connectable / Non-scannable	El dispositivo solo emite paquetes de advertising y no acepta conexiónes ni respuestas a *scan requests*. Es tipico de balizas (*beacons*) que simplemente difunden informacion.
Bonded	El dispositivo BLE ya esta emparejado (*bonded*) con el telefono. Se han intercambiado y almacenado claves, lo que permite establecer enlaces cifrados y con mayor nivel de seguridad.
Legacy Pairing	Indica que el dispositivo utiliza el esquema de emparejamiento BLE clasico (anterior a *LE Secure Connections*). Este metodo ofrece una seguridad inferior frente a ataques de tipo MITM o escuchas pasivas.
LE Secure Connections	El dispositivo soporta el metodo moderno de emparejamiento *LE Secure Connections*, que mejora la proteccion frente a ataques criptograficos y MITM, proporcionando un nivel de seguridad mas elevado.
Public / Random Static / RPA / NRPA	Tipo de dirección BLE utilizada: *Public* (MAC fija, rastreable), *Random Static* (aleatoria pero fija mientras el dispositivo no reinicie), *RPA* o *Resolvable Private Address* (aleatoria, pero resoluble unicamente por dispositivos emparejados mediante IRK) y *NRPA* o *Non-Resolvable Private Address* (aleatoria no resoluble, maxima privacidad pero funcionalidad limitada de conexión).
Advertised Services	Lista de servicios (UUID) anunciados en los paquetes de advertising, por ejemplo `Heart Rate (0x180D)`, `Battery (0x180F)`, `Immediate Alert (0x1802)`, etc. Permiten inferir el tipo de dispositivo y sus capacidades (sensor, wearable, beacon, dispositivo medico, etc.).

- **Exploracion de dispositivos BLE:** Abre nRF Connect y activa el escaneo. Fíjate en la lista de dispositivos cercanos e identifica, para cada uno:
  - Su dirección BLE (Public, Random Static, RPA o NRPA).
  - El nombre que anuncian (si lo tienen).
  - La intensidad de señal (RSSI) y si están cerca o lejos.
  - Las etiquetas que muestra la app: *Nearby*, *Connectable*, *Scannable*, *Find Me*, *Hand Off*, etc.
  - Los servicios que aparecen ya en el advertising (UUIDs visibles sin conectar).

  Elige un dispositivo que sea interesante para seguir la practica.
- **Conexión a un dispositivo BLE:** Toca uno de los dispositivos que soporten conexión (*Connectable*) y conecta. Espera a que nRF Connect termine de descubrir todos los servicios GATT.
- **Inspección de servicios y características GATT:** Explora los servicios que aparecen y mira:
  - Cuales son estándar (UUID de 16 bits).
  - Cuales son propietarios (UUID de 128 bits).
  - Las propiedades de cada característica: `Read`, `Write`, `Write Without Response`, `Notify`, `Indicate`.

  Intenta deducir para que sirve cada servicio según su UUID.
- **Lectura y escritura de características:** Prueba a leer valores de características que lo permitan. Intenta escribir con `Write` o `Write Without Response`. Mira en nRF Logger:
  - Si la escritura ha funcionado o ha dado error.
  - Si aparece algún mensaje de permiso insuficiente (*Insufficient Authentication*, *Write Not Permitted*, etc.).
  - Si la escritura cambia algo en el dispositivo o activa notificaciones.
- Ten nRF Logger abierto mientras haces la practica y revisa estos puntos:
  - Que dirección MAC uso el dispositivo y de que tipo es (Public, Static, RPA, NRPA).
  - Si hubo reintentos de conexión.
  - En que orden se descubrieron los servicios.
  - Si aparecieron errores durante las operaciones GATT.
  - Si se recibieron notificaciones o indicaciones.

Conceptos adicionales para el análisis de dispositivos BLE

Negociación de MTU en BLE. La MTU (*Maximum Transmission Unit*) define el tamaño máximo de datos que pueden enviarse en una sola operación ATT. El valor por defecto es de 23 bytes (20 bytes útiles), pero la MTU puede ampliarse mediante una negociación automática entre cliente y servidor tras la conexión. En el LOG interno de nRF Connect suelen aparecer mensajes como *MTU request* y *MTU changed*, que indican que ambas partes han acordado un tamaño mayor. Una MTU alta permite transferencias más rápidas y con menos fragmentación.

Interpretación del error GATT 133. El error **133 (0x85) GATT ERROR** es uno de los más frecuentes en Android. No es un error específico del protocolo, sino un indicador genérico de que la conexión GATT no ha podido completarse. Las causas más habituales incluyen:

- el dispositivo rechaza conexiones no emparejadas;
- el dispositivo está conectado a su aplicación oficial;
- timeouts internos del firmware;
- fallos temporales del *stack* BLE de Android.

En el LOG de nRF Connect suele aparecer seguido de *Disconnected*.

Tabla de permisos GATT. Cada característica BLE tiene un conjunto de permisos que determinan las operaciones permitidas. En la Tabla III se muestran los más comunes.

Permiso	Descripción
R	Lectura permitida (*Read*).
W	Escritura con respuesta (*Write*).
WNR	Escritura sin respuesta (*Write Without Response*).
N	Notificaciones permitidas (*Notify*).
I	Indicaciones permitidas (*Indicate*).

Diferencias entre BLE y BR/EDR. Es importante distinguir entre Bluetooth Low Energy (BLE) y Bluetooth Clásico (BR/EDR), ya que funcionan de forma diferente:

- **BLE**: orientado a bajo consumo, utiliza el modelo GATT/ATT, permite direcciones aleatorias privadas (RPA, NRPA, Static), usa advertising, MTU variable y operaciones de lectura/escritura sobre características.
- **BR/EDR**: orientado a audio y mayor ancho de banda (A2DP, AVRCP, HFP), no utiliza GATT, emplea perfiles clásicos y generalmente usa direcciones públicas.

Perfil Find Me e Immediate Alert Service. El servicio **Immediate Alert (0x1802)** forma parte del *Find Me Profile* definido por Bluetooth SIG. Permite localizar físicamente un dispositivo BLE mediante la característica **Alert Level (0x2A06)**, que puede activar un sonido, vibración o luz cuando recibe un valor de alerta. nRF Connect suele mostrar dispositivos con este perfil con la etiqueta *Find Me* durante el escaneo.

Manufacturer Data en el advertising BLE. Muchos dispositivos BLE incluyen un campo de *Manufacturer Specific Data* en sus paquetes de advertising. Este campo comienza con un identificador de empresa (Company ID) definido por Bluetooth SIG y va seguido de datos propietarios. La interpretación depende del fabricante, pero suele aportar información como:

- el fabricante del dispositivo;
- el modelo o variante de hardware;
- estados internos o indicadores privados;
- información adicional no estandarizada.

La lista oficial de Company IDs puede consultarse en:
`https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers/`

3. Recursos externos recomendados

Para completar esta práctica es posible que necesites consultar información oficial del Bluetooth SIG y de BlueZ. Estas referencias te ayudaran a identificar servicios, interpretar direcciones y analizar la seguridad del dispositivo estudiado.

- **Tablas de UUID estandar (Assigned Numbers):**
  https://www.bluetooth.com/specifications/assigned-numbers/
- **Tipos de direcciones BLE (Public, Static, RPA, NRPA):**
  https://www.bluetooth.com/blog/bluetooth-device-addresses/
- **Company Identifiers (Manufacturer Data):**
  https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers/
- **Propiedades GATT (Read, Write, Notify, Indicate):**
  https://www.bluetooth.com/specifications/assigned-numbers/generic-attribute-profile/
- **Documentación básica de BlueZ y bluetoothctl:**
  https://git.kernel.org/pub/scm/bluetooth/bluez.git/tree/doc
- **Significado de las etiquetas en nRF Connect:**
  https://github.com/NordicSemiconductor/Android-nRF-Connect
- **Secuencia de conexión y negociación MTU (nRF Logger):**
  https://devzone.nordicsemi.com/