

Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

Prof. Ismael Jiménez Sánchez

**PoC Bettercap BLE Identify & Target
Bluetooth Devices.**

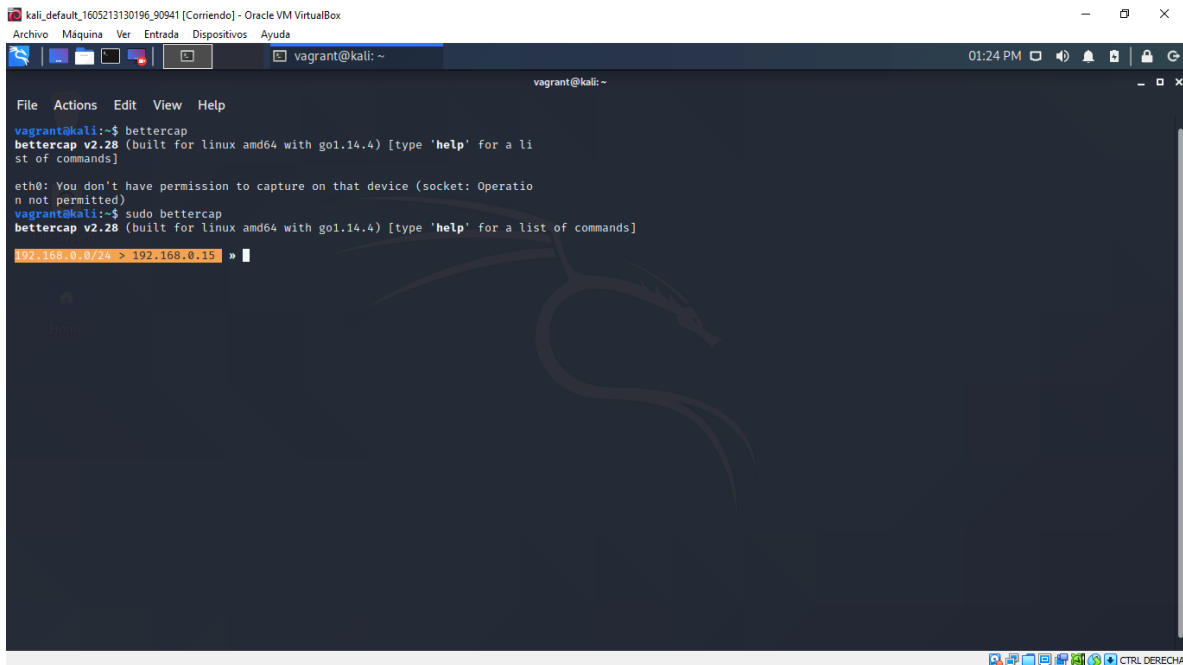
**Alumno(a): Laury del Rosario Mex
Martin**

Ciclo Agosto- Diciembre 2020B

En este PoC vamos poder Identificar y apuntar a dispositivos bluetooth, podremos ver el numero de modelo ya sea celular o cualquier otro dispositivo al igual que el porcentaje de batería que tiene, y también se puede escribir algunos datos en el dispositivo. Pero en lo que nos vamos a enfocar solo será en ver el numero de modelo y el porcentaje de batería del dispositivo atacado. Cabe destacar que es una navaja suiza para redes de 2 a 11 bluetooth de baja energía y ethernet.

PASO 1 Iniciar el Bettercap

Ingresamos a bettercap con el comando ***bettercap***.



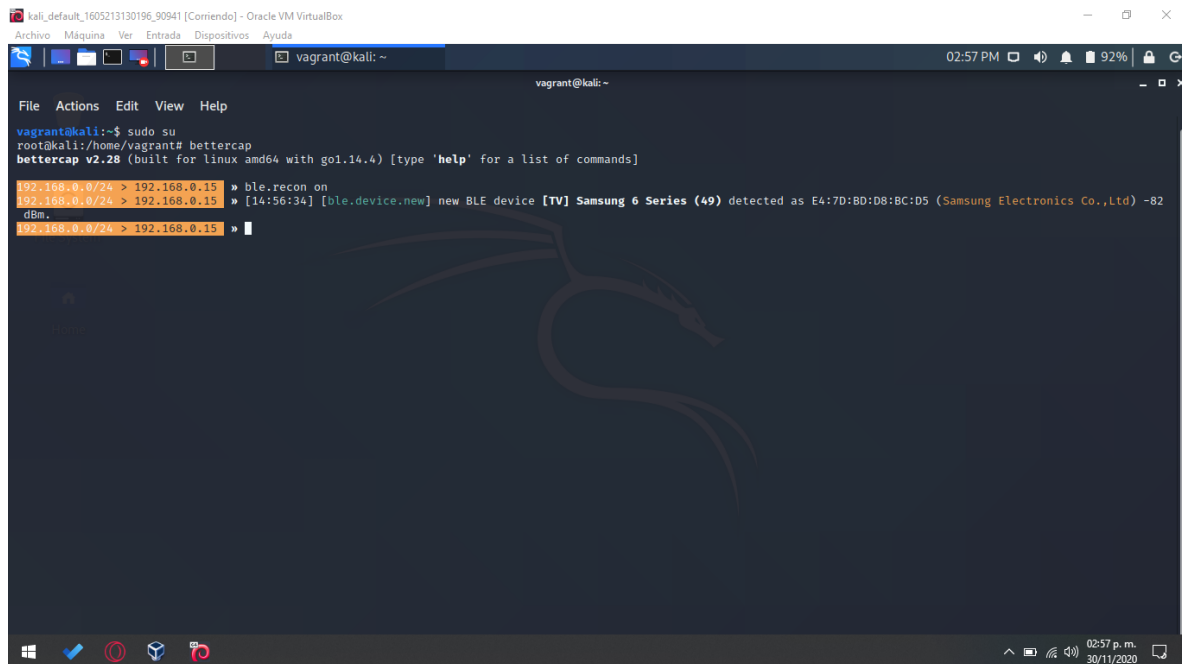
```
kali_default_1605213130196_90941 [Corriendo] - Oracle VM VirtualBox
Archivo  Maquina  Ver  Entrada  Dispositivos  Ayuda
vagrant@kali: ~
01:24 PM

File  Actions  Edit  View  Help
vagrant@kali:~$ bettercap
bettercap v2.28 (built for linux amd64 with go1.14.4) [type 'help' for a list of commands]

eth0: You don't have permission to capture on that device (socket: Operation not permitted)
vagrant@kali:~$ sudo bettercap
bettercap v2.28 (built for linux amd64 with go1.14.4) [type 'help' for a list of commands]
192.168.0.0/24 -> 192.168.0.15 >
```

Paso 2: Ejecutamos el modulo de rastreo de Bluetooth

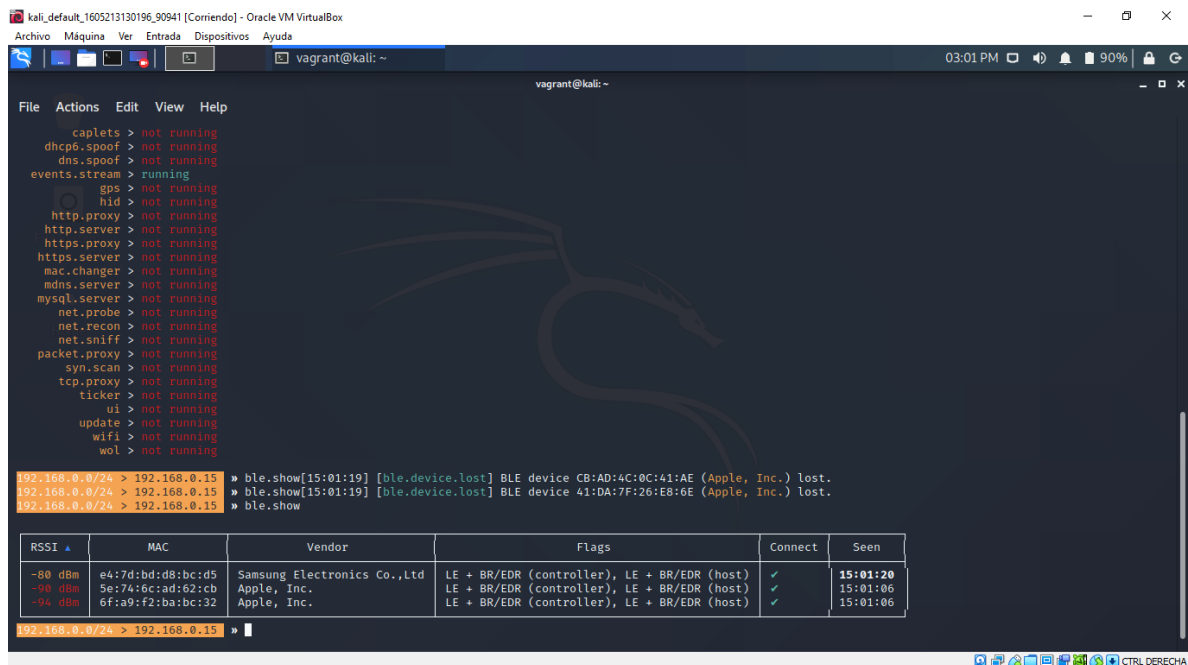
Para empezar el reconocimiento de Bluetooth ponemos el comando ***ble.recon on***



```
kali_default_160521310196_90941 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
vagrant@kali: ~
File Actions Edit View Help
vagrant@kali:~$ sudo su
root@kali:/home/vagrant# bettercap
bettercap v2.28 (built for linux amd64 with go1.14.4) [type 'help' for a list of commands]
192.168.0.0/24 > 192.168.0.15 > ble.recon on
192.168.0.0/24 > 192.168.0.15 > [14:56:34] [ble.device.new] new BLE device [TV] Samsung 6 Series (49) detected as E4:7D:BD:D8:BC:D5 (Samsung Electronics Co.,Ltd) -82 dBm.
192.168.0.0/24 > 192.168.0.15 > |
```

Paso 3: Identificamos los dispositivos

Para ver los dispositivos de una mejor manera se utiliza el comando ***ble.show***



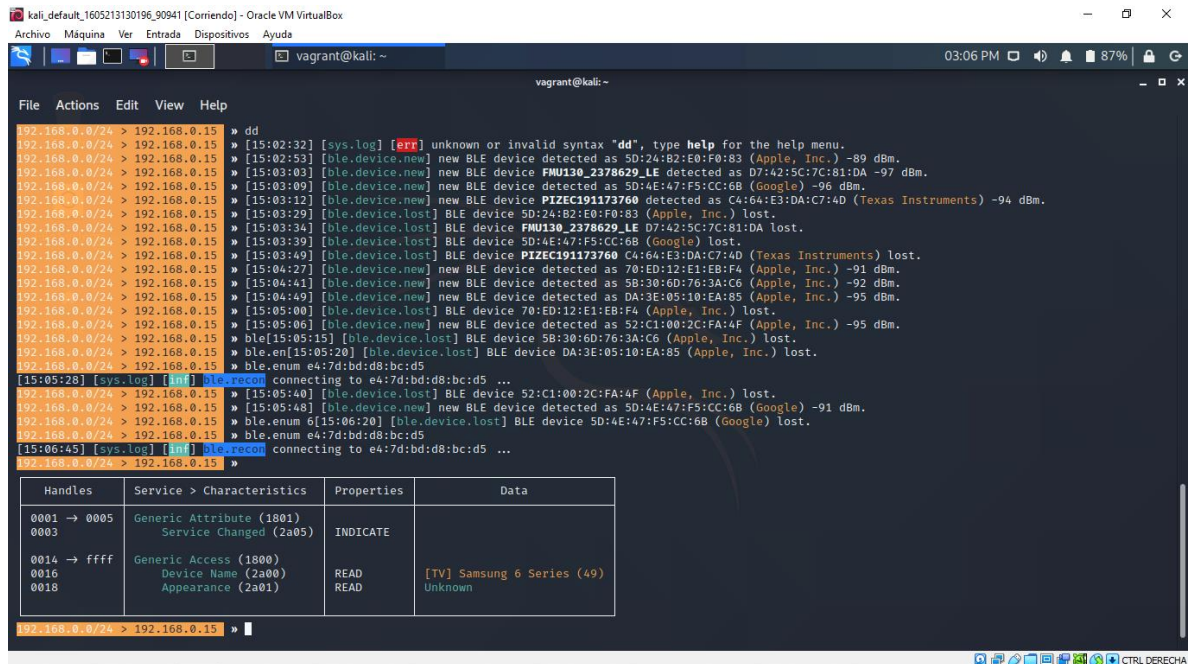
```
kali_default_160521310196_90941 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
vagrant@kali: ~
File Actions Edit View Help
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
net.probe > not running
net.recon > not running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running
192.168.0.0/24 > 192.168.0.15 > ble.show[15:01:19] [ble.device.lost] BLE device CB:AD:4C:0C:41:AE (Apple, Inc.) lost.
192.168.0.0/24 > 192.168.0.15 > ble.show[15:01:19] [ble.device.lost] BLE device 41:DA:7F:26:E8:6E (Apple, Inc.) lost.
192.168.0.0/24 > 192.168.0.15 > ble.show
```

RSSI	MAC	Vendor	Flags	Connect	Seen
-80 dBm	e4:7d:bd:d8:bc:d5	Samsung Electronics Co.,Ltd	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	15:01:20
-90 dBm	5e:74:6c:ad:62:cb	Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	15:01:06
-94 dBm	6f:a9:f2:ba:bc:32	Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	15:01:06

```
192.168.0.0/24 > 192.168.0.15 > |
```

Paso 4: Interactuamos y escaneamos el dispositivo

Para dirigir el escaneo a un dispositivo vamos a usar el comando **ble.enum mac** *addres*.



```
kali_default_160521310196_90941 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

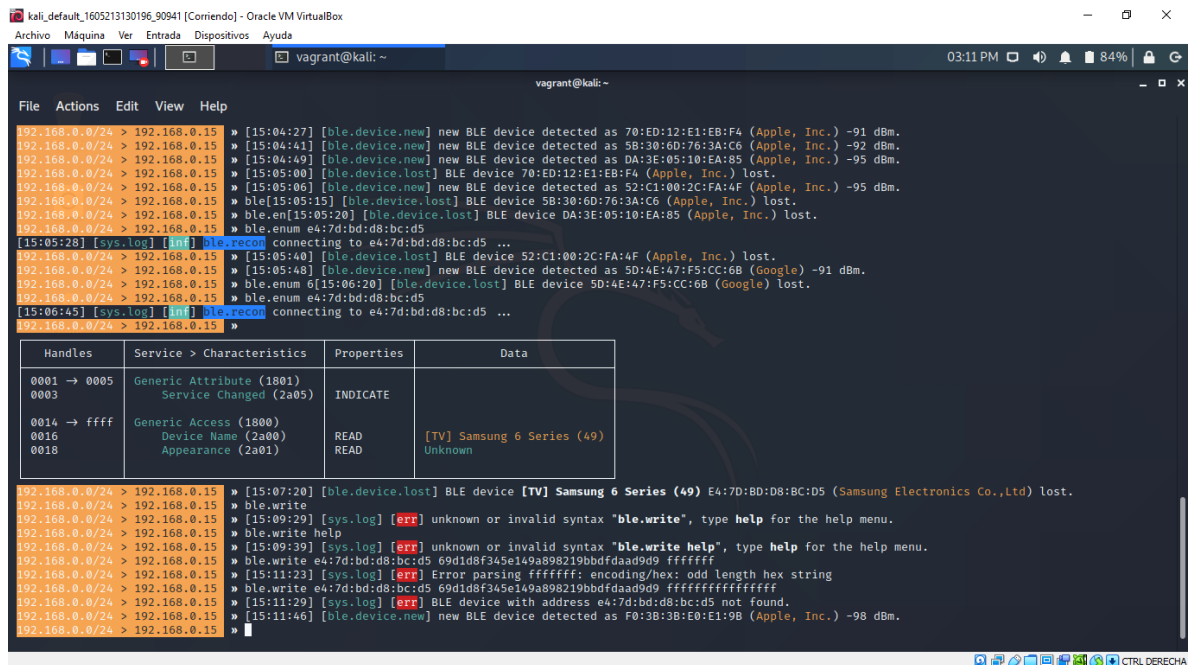
vagrant@kali: ~
File Actions Edit View Help

192.168.0.0/24 > 192.168.0.15 > dd
[15:02:32] [sys.log] [err] unknown or invalid syntax "dd", type help for the help menu.
[15:02:53] [ble.device.new] new BLE device detected as 5D:24:B2:E0:F0:83 (Apple, Inc.) -89 dBm.
[15:03:03] [ble.device.new] new BLE device FMU130_2378629_LE detected as D7:42:5C:7C:81:DA -97 dBm.
[15:03:09] [ble.device.new] new BLE device detected as 5D:4E:47:F5:CC:6B (Google) -96 dBm.
[15:03:12] [ble.device.new] new BLE device PIZEC191173760 detected as C4:64:E3:DA:C7:4D (Texas Instruments) -94 dBm.
[15:03:29] [ble.device.lost] BLE device 5D:24:B2:E0:F0:83 (Apple, Inc.) lost.
[15:03:34] [ble.device.lost] BLE device FMU130_2378629_LE D7:42:5C:7C:81:DA lost.
[15:03:39] [ble.device.lost] BLE device 5D:4E:47:F5:CC:6B (Google) lost.
[15:03:49] [ble.device.lost] BLE device PIZEC191173760 C4:64:E3:DA:C7:4D (Texas Instruments) lost.
[15:04:27] [ble.device.new] new BLE device detected as 70:ED:12:E1:EB:F4 (Apple, Inc.) -91 dBm.
[15:04:41] [ble.device.new] new BLE device detected as 58:30:6D:76:3A:C6 (Apple, Inc.) -92 dBm.
[15:04:49] [ble.device.new] new BLE device detected as DA:3E:05:10:EA:85 (Apple, Inc.) -95 dBm.
[15:05:00] [ble.device.lost] BLE device 70:ED:12:E1:EB:F4 (Apple, Inc.) lost.
[15:05:06] [ble.device.new] new BLE device detected as 52:C1:00:2C:FA:4F (Apple, Inc.) -95 dBm.
[15:05:15] [ble.device.lost] BLE device 58:30:6D:76:3A:C6 (Apple, Inc.) lost.
[15:05:20] [ble.device.lost] BLE device DA:3E:05:10:EA:85 (Apple, Inc.) lost.
[15:05:28] [sys.log] [inf] ble.recon connecting to e4:7d:bd:d8:bc:d5 ...
[15:05:40] [ble.device.lost] BLE device 52:C1:00:2C:FA:4F (Apple, Inc.) lost.
[15:05:48] [ble.device.new] new BLE device detected as 5D:4E:47:F5:CC:6B (Google) -91 dBm.
[15:06:20] [ble.device.lost] BLE device 5D:4E:47:F5:CC:6B (Google) lost.
[15:06:45] [sys.log] [inf] ble.recon connecting to e4:7d:bd:d8:bc:d5 ...

Handles Service > Characteristics Properties Data
0001 -> 0005 Generic Attribute (1801) INDICATE
0003 Service Changed (2a05)
0014 -> ffff Generic Access (1800)
0016 Device Name (2a00) READ [TV] Samsung 6 Series (49)
0018 Appearance (2a01) READ Unknown

192.168.0.0/24 > 192.168.0.15 > |
```

Podemos escribir el valor de "ffffffffffffff" en ese dispositivo escribiendo el comando **ble.write TheMacAddress TheFieldToWriteTo ValueToWrite**.



```
kali_default_160521310196_90941 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

vagrant@kali: ~
File Actions Edit View Help

192.168.0.0/24 > 192.168.0.15 > [15:04:27] [ble.device.new] new BLE device detected as 70:ED:12:E1:EB:F4 (Apple, Inc.) -91 dBm.
192.168.0.0/24 > 192.168.0.15 > [15:04:41] [ble.device.new] new BLE device detected as 58:30:6D:76:3A:C6 (Apple, Inc.) -92 dBm.
192.168.0.0/24 > 192.168.0.15 > [15:04:49] [ble.device.new] new BLE device detected as DA:3E:05:10:EA:85 (Apple, Inc.) -95 dBm.
192.168.0.0/24 > 192.168.0.15 > [15:05:00] [ble.device.lost] BLE device 70:ED:12:E1:EB:F4 (Apple, Inc.) lost.
192.168.0.0/24 > 192.168.0.15 > [15:05:06] [ble.device.new] new BLE device detected as 52:C1:00:2C:FA:4F (Apple, Inc.) -95 dBm.
192.168.0.0/24 > 192.168.0.15 > [15:05:15] [ble.device.lost] BLE device 58:30:6D:76:3A:C6 (Apple, Inc.) lost.
192.168.0.0/24 > 192.168.0.15 > [15:05:20] [ble.device.lost] BLE device DA:3E:05:10:EA:85 (Apple, Inc.) lost.
192.168.0.0/24 > 192.168.0.15 > [15:05:28] [sys.log] [inf] ble.recon connecting to e4:7d:bd:d8:bc:d5 ...
192.168.0.0/24 > 192.168.0.15 > [15:05:40] [ble.device.lost] BLE device 52:C1:00:2C:FA:4F (Apple, Inc.) lost.
192.168.0.0/24 > 192.168.0.15 > [15:05:48] [ble.device.new] new BLE device detected as 5D:4E:47:F5:CC:6B (Google) -91 dBm.
192.168.0.0/24 > 192.168.0.15 > [15:06:20] [ble.device.lost] BLE device 5D:4E:47:F5:CC:6B (Google) lost.
192.168.0.0/24 > 192.168.0.15 > [15:06:45] [sys.log] [inf] ble.recon connecting to e4:7d:bd:d8:bc:d5 ...
192.168.0.0/24 > 192.168.0.15 >

Handles Service > Characteristics Properties Data
0001 -> 0005 Generic Attribute (1801) INDICATE
0003 Service Changed (2a05)
0014 -> ffff Generic Access (1800)
0016 Device Name (2a00) READ [TV] Samsung 6 Series (49)
0018 Appearance (2a01) READ Unknown

192.168.0.0/24 > 192.168.0.15 > [15:07:20] [ble.device.lost] BLE device [TV] Samsung 6 Series (49) E4:7D:BD:D8:BC:D5 (Samsung Electronics Co.,Ltd) lost.
192.168.0.0/24 > 192.168.0.15 > ble.write
192.168.0.0/24 > 192.168.0.15 > [15:09:29] [sys.log] [err] unknown or invalid syntax "ble.write", type help for the help menu.
192.168.0.0/24 > 192.168.0.15 > ble.write help
192.168.0.0/24 > 192.168.0.15 > [15:09:39] [sys.log] [err] unknown or invalid syntax "ble.write help", type help for the help menu.
192.168.0.0/24 > 192.168.0.15 > ble.write e4:7d:bd:d8:bc:d5 69d1d8f345e149a898219bbdfdaad9d9 ffffffff
192.168.0.0/24 > 192.168.0.15 > [15:11:23] [sys.log] [err] Error parsing ffffffff: encoding/hex: odd length hex string
192.168.0.0/24 > 192.168.0.15 > ble.write e4:7d:bd:d8:bc:d5 69d1d8f345e149a898219bbdfdaad9d9 ffffffff
192.168.0.0/24 > 192.168.0.15 > [15:11:29] [sys.log] [err] BLE device with address e4:7d:bd:d8:bc:d5 not found.
192.168.0.0/24 > 192.168.0.15 > [15:11:46] [ble.device.new] new BLE device detected as F0:3B:3B:E0:E1:9B (Apple, Inc.) -98 dBm.
192.168.0.0/24 > 192.168.0.15 > |
```

Pero como podemos ver no me dejo hacerlo.