

Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1: Разобрать дамп hci-соединения. Указать, к какому устройству осуществлялся доступ, увенчался ли он успехом, назвать имя устройства, класс и смещение времени. Отчет должен содержать информацию об адресе, имени, смещении во времени и наличии доступа за время дампа.

Открываю и просматриваю в веершарке дамп:

No.	Time	Source	Destination	Protocol	Length	TCP Flags	Info
21	71.107757	controller	host	HCI_EVT	10		Rcvd Local Remote Connection Result
22	71.107757	host	controller	HCI_CMD	14		Sent Remote Name Request
23	71.107777	localhost ()	AsustekC_0c:4a:ca ()	L2CAP	15		Sent Information Request (Extend)
24	71.107787	localhost ()	AsustekC_0c:4a:ca ()	L2CAP	21		Sent Information Response (Extend)
25	71.111442	controller	host	HCI_EVT	7		Rcvd Command Status (Remote Name)
26	71.183323	controller	host	HCI_EVT	258		Rcvd Remote Name Request Complete
27	71.196868	AsustekC_0c:4a:ca (ASUS_Z00LD)	localhost ()	L2CAP	21		Rcvd Information Response (Extend)
28	71.197363	AsustekC_0c:4a:ca (ASUS_Z00LD)	localhost ()	L2CAP	15		Rcvd Information Request (Fixed)
29	71.197437	localhost ()	AsustekC_0c:4a:ca (ASUS_Z00LD)	L2CAP	15		Sent Information Request (Fixed)
30	71.197445	localhost ()	AsustekC_0c:4a:ca (ASUS_Z00LD)	L2CAP	25		Sent Information Response (Fixed)
31	71.226810	controller	host	HCI_EVT	8		Rcvd Number of Completed Packets
32	71.228538	AsustekC_0c:4a:ca (ASUS_Z00LD)	localhost ()	L2CAP	25		Rcvd Information Response (Fixed)
33	73.138864	host	controller	HCI_CMD	7		Sent Disconnect
34	73.143530	controller	host	HCI_EVT	7		Rcvd Command Status (Disconnect)

[Last Role Change in Frame: 12]
[Current Mode: Active Mode (0)]
[Last Mode Change in Frame: 13]

▼ Bluetooth L2CAP Protocol

Length: 6
CID: L2CAP Signaling Channel (0x0001)

▼ Command: Information Request
 Command Code: Information Request (0x0a)
 Command Identifier: 0x01
 Command Length: 2
 Information Type: Extended Features Mask (0x0002)

0000	02	0b	20	0a	00	06	00	01	00	0a	01	02	00	02	00

Есть выполнение мультиплексирования локальных соединений. Передача данных на устройство Asustek - мобильный телефон. Непосредственно данных в дампе не обнаружено, в основном служебный обмен пакетами. Смотрим остальные данные:

No.	Time	Source	Destination	Protocol	Length	TCP Flags	Info
208	160.817358	AsustekC_0c:4a:ca (ASUS_Z00LD)	localhost ()	L2CAP	21		Rcvd Information Response (E
209	160.817516	localhost ()	AsustekC_0c:4a:ca (ASUS_Z00LD)	L2CAP	15		Sent Information Request (F
210	160.818831	AsustekC_0c:4a:ca (ASUS_Z00LD)	localhost ()	L2CAP	15		Rcvd Information Request (F
211	160.819086	localhost ()	AsustekC_0c:4a:ca (ASUS_Z00LD)	L2CAP	25		Sent Information Response (F
212	160.824104	AsustekC_0c:4a:ca (ASUS_Z00LD)	localhost ()	L2CAP	25		Rcvd Information Response (F

Frame 211: 25 bytes on wire (200 bits), 25 bytes captured (200 bits)
Encapsulation type: Bluetooth H4 with linux header (99)
Arrival Time: Jul 17, 2018 23:32:43.602430000 MSK
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1531859563.602430000 seconds
[Time delta from previous captured frame: 0.000255000 seconds] ← delta
[Time delta from previous displayed frame: 0.000255000 seconds]
[Time since reference or first frame: 160.819086000 seconds]
Frame Number: 211
Frame Length: 25 bytes (200 bits)
Capture Length: 25 bytes (200 bits)
[Frame is marked: False]
[Frame is ignored: False]
Point-to-Point Direction: Sent (0)
[Protocols in frame: bluetooth:hci_h4:bthci_acl:bt2cap]
Bluetooth
[Source: 00:00:00:00:00:00 (00:00:00:00:00:00)] ← mac local
[Destination: AsustekC_0c:4a:ca (2c:56:dc:0c:4a:ca)] ← mac local
Bluetooth HCI H4
[Direction: Sent (0x00)]

Привлекает внимание MAC адрес локалхоста. На всей дистанции дампа было несколько успешных попыток соединения и обменом информацией:

Time	Source	Destination	Protocol	Length	TC	Info
146.584794	host	controller	HCI_CMD	6		Sent Read Remote Supported Features
146.587693	controller	host	HCI_EVT	6		Rcvd Max Slots Change
146.591285	controller	host	HCI_EVT	7		Rcvd Command Status (Read Remote Supported Features)
146.594150	controller	host	HCI_EVT	14		Rcvd Read Remote Supported Features
146.594360	host	controller	HCI_CMD	7		Sent Read Remote Extended Features
146.598062	controller	host	HCI_EVT	7		Rcvd Command Status (Read Remote Extended Features)
146.605941	host	controller	HCI_CMD	6		Sent Change Connection Link Key
146.610163	controller	host	HCI_EVT	7		Rcvd Command Status (Change Connection Link Key)
146.612726	controller	host	HCI_EVT	6		Rcvd Change Connection Link Key Complete
146.673442	controller	host	HCI_EVT	16		Rcvd Read Remote Extended Features Complete
146.673632	host	controller	HCI_CMD	14		Sent Remote Name Request
146.673673	localhost ()	AsustekC_0c:4a:ca (AS...	L2CAP	15		Sent Information Request (Extended Features Mask)
146.678388	controller	host	HCI_EVT	7		Rcvd Command Status (Remote Name Request)
146.814256	AsustekC_0c:4a:ca (ASU...	localhost ()	L2CAP	21		Rcvd Information Response (Extended Features Mask, Success)
146.814402	localhost ()	AsustekC_0c:4a:ca (AS...	L2CAP	15		Sent Information Request (Fixed Channels Supported)
146.820055	AsustekC_0c:4a:ca (ASU...	localhost ()	L2CAP	25		Rcvd Information Response (Fixed Channels Supported, Success)
146.857434	controller	host	HCI_EVT	258		Rcvd Remote Name Request Complete
146.958327	controller	host	HCI_EVT	8		Rcvd Number of Completed Packets

Frame 211: 25 bytes on wire (200 bits), 25 bytes captured (200 bits)
Encapsulation type: Bluetooth H4 with linux header (99)
Arrival Time: Jul 17, 2018 23:32:43.602430000 MSK
[Time shift for this packet: 0.000000000 seconds]
Fnch Time: 1531859563.602430000 seconds

Задание 2*: Изучить утилиты для работы с bluetooth. Отчет — скриншоты с результатами исследований.

- hcitool

Активирует Bluetooth сервис:

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

```
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/blueuetooth.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:~#
```

Запуская сканирование нескрытых bluetooth hcitool scan – обнаружено одно устройство (МАК и имя).

Запуская сканирование с выводом более подробной информации hcitool inq – уже получается сдвиг времени и класс устройства

```
root@kali:~# hcitool scan
Scanning ...
EC:D0:9F:D1:33:0A      boris
```

```
root@kali:~# hcitool inq
Inquiring ...
EC:D0:9F:D1:33:0A      clock offset: 0x75dc      class: 0x5a020c
```

- Bluelog

Запустим мониторинг Bluetooth эфира bluelog -v

Видим маки и классы устройств поблизости

```
root@kali: ~
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

Пробую 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^C
root@kali: ~# 
```

- l2ping

Проба утилиты для DoS атаки на Bluetooth-устройство. Сканируется эфир и выбираем свое устройство. Далее

l2ping -i hci0 -s 600 -f <M:A:C>

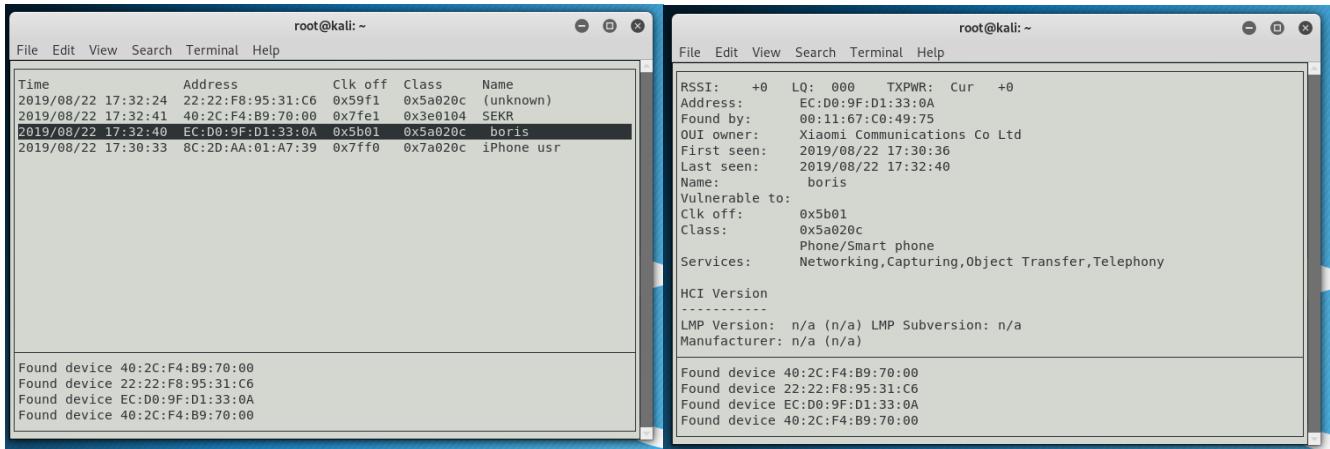
```
root@kali: ~
File Edit View Search Terminal Help
root@kali: ~# hcitool scan
Scanning ...
22:22:F8:95:31:C6      Лизавета
EC:D0:9F:D1:33:0A      boris
20:68:9D:2D:3A:2E      kali
root@kali: ~# hcitool scan
```



```
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 блютуз наушники, запущена музыка. Изменений не произошло, блютуз работал, музыка играла без сбоев.

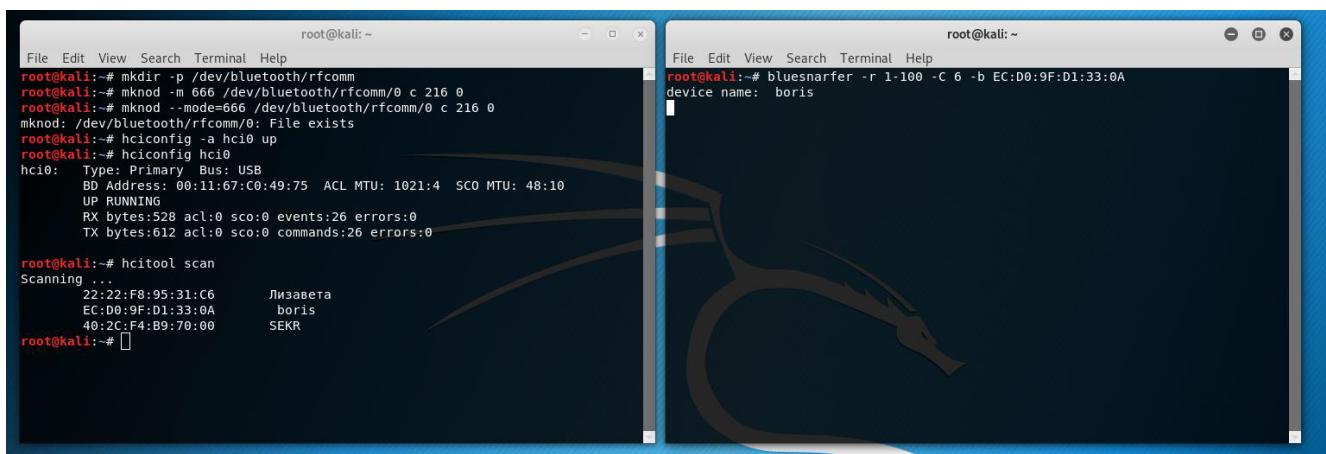
- Btscanner – сканер с GUI интерфейсом для получения расширенной информации о Bluetooth устройствах.



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

Сперва создается виртуальное устройство rfcomm на attack-машине и «наделяется» 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 попытка прочитать из телефонной книги первые 100 номеров)
bluesnarfer -r 1-100 -C 6 -b <M:A:C>



На современных устройствах концепция хранения телефонных книг и распределения памяти сильно изменилась с момента выхода этой утилиты. Данная атака выполнима только на старых телефонах, как пример, nokia 3310. Можно попытаться выполнить AT команды, их структура не поменялась до сих пор.