

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @
TekGyd | itechhacks | Mukeshtricks4u*////////

Okay, I dug this out of the wayback machine. This was a couple posts by Dr_GrEeN on the old forum. We Shouldn't loose this stuff.

Quote Originally Posted by Dr_GrEen

Part1

Hey Guys

Just thought I'd post a little on Bluetooth Hacking because I can see thereis a lot of questions and not alot of answers So here's how I hacked my samsung d600.

First I popped to my local supermarket and picked myself up a bluetooth dongle for 6.99!!!! Because my shitieToshiba Satellite P100 doesn't have bluetooth

Ok first lets configure BT.....

Type :

```
bt ~ # mkdir -p /dev/bluetooth/rfcomm  
mknod -m 666 /dev/bluetooth/rfcomm/0 c 216 0
```

Thats Bluesnarfer done, now for bluebugger.....

Type:

```
bt ~ # mknod --mode=666 /dev/rfcomm0 c 216 0
```

Ok now we can fire up are Bluetooth adaptor, so type:

```
bt ~ # hciconfig hci0 up
```

Now are bluetooth adaptor should be ready, check by typing :

```
bt ~ # hciconfig hci0
```

and you should see something like this:

```
hci0: Type: USB  
BD Address: 00:11:22:33:44:55 ACL MTU: 678:8 SCO MTU: 48:10  
UP RUNNING  
RX bytes:85 acl:0 sco:0 events:9 errors:0  
TX bytes:33 acl:0 sco:0 commands:9 errors:0
```

Ok now we are ready to scan so type:

```
bt ~ # hcitool scan hci0
```

And you should see all the devices in the area. You can also use btscanner and btscanner has a bruteforce scanner for discovering hidden devices.

Now note the name and MAC of the target and let's move on.

First thing lets try to ping are target. Type:

```
l2ping <target MAC>
```

If you dont get a ping GOOD LUCK

Next we need to find out a little about the device we want to hack so lets fire up blueprint.

And type:

```
sdptools browse --tree --l2cap <target MAC>
```

And you should get something like this:

Code:

```
Browsing 00:16:DB:A1:B6:B9 ...
Attribute Identifier : 0x0 - ServiceRecordHandle
  Integer : 0x10000
Attribute Identifier : 0x1 - ServiceClassIDList
  Data Sequence
    UUID128 : 0xdb1d8f12-95f3-402c-9b97-bc504c9a-55c4
Attribute Identifier : 0x4 - ProtocolDescriptorList
  Data Sequence
    Data Sequence
      UUID16 : 0x0100 - L2CAP
    Data Sequence
      UUID16 : 0x0003 - RFCOMM
      Channel/Port (Integer) : 0x1
Attribute Identifier : 0x5 - BrowseGroupList
  Data Sequence
    UUID16 : 0x1002 - PublicBrowseGroup
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
  Data Sequence
    Code ISO639 (Integer) : 0x656e
    Encoding (Integer) : 0x6a
    Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
  Data Sequence
    Data Sequence
      UUID128 : 0x1cdb1d8f-1295-f340-2c9b-97bc504c-9a55
      Version (Integer) : 0x100
Attribute Identifier : 0x100
  Data : 57 42 54 45 58 54 00 00
Attribute Identifier : 0x8003
  Integer : 0x1
```

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10001

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence

UUID16 : 0x1101 - SerialPort

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x0100 - L2CAP

Data Sequence

UUID16 : 0x0003 - RFCOMM

Channel/Port (Integer) : 0x2

Attribute Identifier : 0x5 - BrowseGroupList

Data Sequence

UUID16 : 0x1002 - PublicBrowseGroup

Attribute Identifier : 0x9 - BluetoothProfileDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x1101 - SerialPort

Version (Integer) : 0x100

Attribute Identifier : 0x100

Data : 53 65 72 69 61 6c 20 50 6f 72 74 00 00

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10002

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence

UUID16 : 0x1103 - DialupNetworking (DUN)

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x0100 - L2CAP

Data Sequence

UUID16 : 0x0003 - RFCOMM

Channel/Port (Integer) : 0x3

Attribute Identifier : 0x5 - BrowseGroupList

Data Sequence

UUID16 : 0x1002 - PublicBrowseGroup

Attribute Identifier : 0x9 - BluetoothProfileDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x1103 - DialupNetworking (DUN)

Version (Integer) : 0x100

Attribute Identifier : 0x100

Data : 44 69 61 6c 2d 75 70 20 4e 65 74 77 6f 72 6b 69 6e 67 00 00

Attribute Identifier : 0x305

Integer : 0x0

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10003

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence

UUID16 : 0x1112 - HeadsetAudioGateway

UUID16 : 0x1203 - GenericAudio

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x0100 - L2CAP

Data Sequence

UUID16 : 0x0003 - RFCOMM

Channel/Port (Integer) : 0x4

Attribute Identifier : 0x5 - BrowseGroupList

Data Sequence

UUID16 : 0x1002 - PublicBrowseGroup

Attribute Identifier : 0x9 - BluetoothProfileDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x1108 - Headset

Version (Integer) : 0x100

Attribute Identifier : 0x100

Data : 56 6f 69 63 65 20 47 57 00 00

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10004

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence

UUID16 : 0x111f - HandsfreeAudioGateway

UUID16 : 0x1203 - GenericAudio

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x0100 - L2CAP

Data Sequence

UUID16 : 0x0003 - RFCOMM

Channel/Port (Integer) : 0x5

Attribute Identifier : 0x5 - BrowseGroupList

Data Sequence

UUID16 : 0x1002 - PublicBrowseGroup

Attribute Identifier : 0x9 - BluetoothProfileDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x111e - Handsfree

Version (Integer) : 0x101

Attribute Identifier : 0x100

Data : 56 6f 69 63 65 20 47 57 00 00

Attribute Identifier : 0x301

Integer : 0x1

Attribute Identifier : 0x311

Integer : 0x1

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10005

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence

UUID16 : 0x110a - AudioSource

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x0100 - L2CAP
Channel/Port (Integer) : 0x19
Data Sequence
UUID16 : 0x0019 - AVDTP
Channel/Port (Integer) : 0x100
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x110d - AdvancedAudio
Version (Integer) : 0x100
Attribute Identifier : 0x100
Data : 41 64 76 61 6e 63 65 64 20 61 75 64 69 6f 20 73 6f 75 72 63 65 00 00
Attribute Identifier : 0x311
Integer : 0x1

Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10006

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence
UUID16 : 0x110c - RemoteControlTarget

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Channel/Port (Integer) : 0x17
Data Sequence
UUID16 : 0x0017 - AVCTP
Channel/Port (Integer) : 0x100

Attribute Identifier : 0x5 - BrowseGroupList

Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup

Attribute Identifier : 0x9 - BluetoothProfileDescriptorList

Data Sequence
Data Sequence
UUID16 : 0x110e - RemoteControl
Version (Integer) : 0x100

Attribute Identifier : 0x311

Integer : 0x100

Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10007

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x6

Data Sequence
 UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
 UUID16 : 0x1002 - PublicBrowseGroup
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
 Data Sequence
 UUID16 : 0x1106 - OBEXFileTransfer
 Version (Integer) : 0x100
Attribute Identifier : 0x100
Data : 4f 42 45 58 20 46 69 6c 65 20 54 72 61 6e 73 66 65 72 00 00

Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10008
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
 UUID16 : 0x1105 - OBEXObjectPush
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
 Data Sequence
 UUID16 : 0x0100 - L2CAP
Data Sequence
 UUID16 : 0x0003 - RFCOMM
 Channel/Port (Integer) : 0x7
Data Sequence
 UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
 UUID16 : 0x1002 - PublicBrowseGroup
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
 Data Sequence
 UUID16 : 0x1105 - OBEXObjectPush
 Version (Integer) : 0x100
Attribute Identifier : 0x100
Data : 4f 62 6a 65 63 74 20 50 75 73 68 00 00
Attribute Identifier : 0x303
Data Sequence
 Integer : 0x1
 Integer : 0x3
 Integer : 0x5
 Integer : 0xff

Now if you asked me what does this mean I wouldn't know, but I think it tells you abit about the channels and what services are running on what channel.

Anyway after playing abit I found that my D600 uses channel 7 for phonebook lookup etc. I think every make and model is diffrent so you might have to try a few until you get the right one. Like I said im only just getting to grips with linux So if anybodu knows anymore I'd love to read about it.