脱壳基础(调试修改内存)

■ 加壳脱壳第一天.rar

这个程序的demo我给弄丢了。

应该就是

一个按钮,监听事件是实现加法

再写一个减法函数。但不调用

我们做的就是希望在内存中找到你法函数指令,修改为减去的。

以在脑中建立,内存可修改的概念。

1.运行程序



2.运行android_servers

```
■ 管理员: C:\Windows\System32\cmd.exe - adb shell
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
D:\>adb shell
root@generic:/ # su
root@generic:/data/local/tmp # ls -l
-rwxrwxrwx root
                 root
                           523480 2015-04-13 06:35 android_server
                          rw-rw-rw- root
                 root
-rw-rw-rw- root
                                0 2016-07-07 05:55 com.example.laiwenjie.arm
                 root
                                 2016-07-07 05:55 11db
drwxrwxr-x root
                 root
-rw-rw-rw- root
                 root
                          9399052 2016-06-28 10:50 11db-server
                             1428 2016-06-28 10:50 start_lldb_server.sh
-rw-rw-rw- root
                 root
root@generic:/data/local/tmp # ./android_server
IDA Android 32-bit remote debug server(ST) v1.19. Hex-Rays (c) 2004-2015
Listening on port #23946...
```

3.转发端口

adb forward tcp:23946 tcp:23946

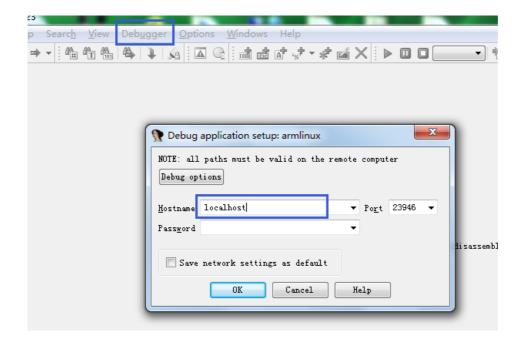
```
面 管理员:C:\Windows\System32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

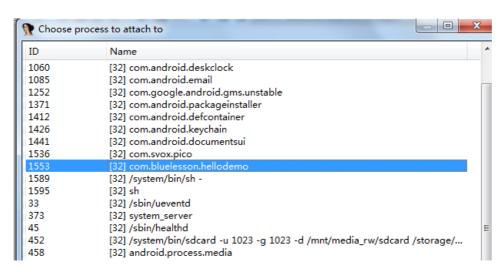
D:\>adb forward tcp:23946 tcp:23946

D:\>
```

4.IDA附加调试

注意程序位数:32位 如果不对应获取不到进程模块





5.ctrl+s获取模块信息,获得基址

Choose segment to jump	· •	HAPTING IN THE DA	n novi							
Name	Start	End	R	W	Х	D	L	Align	Base	Туре
(stack:1569)	A8986000	A8A83000	R	W		D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8A83000	A8B59000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8B59000	A8B5A000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8B5A000	A8B65000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8B65000	A8B66000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8B66000	A8B68000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8B68000	A8B69000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8B69000	A8BBF000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8BBF000	A8BC2000	R			D		byte	00	public
data@app@com.bluelesson.hellodemo_1.apk@classes.dex	A8BC2000	A8CF1000	R			D		byte	00	public
debug002	A8CF1000	A8CF2000				D		byte	00	public
(stack:1568)	A8CF2000	A8DEF000	R	W		D		byte	00	public
debug003	A8DEF000	A8DF0000				D		byte	00	public
⊕ [stack:1567]	A8DF0000	A8EED000	R	W		D		byte	00	public
binder binder	A8EED000	A8FEB000	R			D		byte	00	public
debug004	A8FEB000	A8FEC000				D		byte	00	public
E. Liscon	*0000000	*******	-	147		-		17.	00	100

6 找到dex基址

```
Hex View-3
A8A83008
          0028 0000 1A94 0026
                               .....)
A8A83818
          1ACO 0026 0373 0000
                                ...8.5...
A8A83018
          1E38 0026 C018 0000
                                8.8....
A8A83020
          0000 0000 B2C7 6DD2
                                . . . . . . . m
          6564 0A78 3330 0035
A8A83028
                                dex.035.
A8A83030
          26AC 482E 563E 526D
                                .&.H>UmR
A8A83038
          D010 4E6A 427E 0DBF
                                ..jN~B..
A8A83040 DDBC AFE8 E666 0C2F
                                ....f./.
A8A83048
          1494 0026 0070 0000
                                ...&.p....
A8A83050 5678 1234 0000 0000
                               x04.....
A8A83058 0000 0000 824C 0006
                                ....L...
```

用另一个IDA找到函数偏移地址

```
PopupWindowCompat$Api23PopupWindowImpl_getW

| PopupWindowCompat$Api23PopupWindowImpLgetW
| PopupWindowCompat$Api23PopupWindowImpLsetO\
| PopupWindowCompat$Api23PopupWindowImpLsetWi
| TextViewCompat$Api23TextViewCompatImpl_init_@V
                                                            CODE: 8813E86C
                                                                                             moue-result
                                                                                                                                បផ
                                                            CODE: 0013F86E
                                                            CODE:0013E86E locret:
                                                                                                                       # CODE XREF: MainActivi
                                                                                              .line 21
TextViewCompat$Api23TextViewCompatImpl_setTextAp
                                                            CODE:0013F86E
                                                                                             return
                                                                                                                                vΘ
   ActionBarActivity init @V
f AppCompatDelegateImplV23_init_@VLLL f AppCompatDelegateImplV23_mapNightMode@II
                                                            CODE: 0013E870
                                                            CODE 00135870 loc_135870
                                                                                                                         CODE XREE: MainActivi
AppcompatDelegateImplV23_wr.
f AppCompatDelegateImplV23_wr.
f MainActivity_init_@V
f MainActivity_init_@VLL
f MainActivity_access$super@LLLL
  AppCompatDelegateImplV23_wrapWindowCallback@L
MainActivity_init_@V
                                                            CODE: 0013F870
                                                                                             sub-int
                                                                                                                                v0, a, b
locret
                                                            CODE: 0013F874
                                                                                             goto
                                                            CODE:0013F874 Method End
                                                            CODE:0013F874 #
MainActivity_Add@III
MainActivity_Sub@III
                                                            CODE:0013F876
                                                                                              .byte
                                                            CODE:0013F877
                                                                                              .byte
f MainActivity_onClick@VL
f MainActivity_onCreate@VL
                                                            CODE:0013F878 #
                                                            CODE:0013F878 # Method 16373
CODE:0013F878 word_13F878:
                                                                                            (0x3ff5)
f DrawableCompat$LollipopDrawableImpl_init_@V
f DrawableCompat$LollipopDrawableImpl_applyThem
                                                                                                                        # DATA XREF: CODE:0008A
                                                                                             .short 8
                                                            CODE:0013F878
                                                                                                                       # Number of registers :
   DrawableCompat$LollinonDrawableImpl_canApplyThe
减逐数对应的指令
0013F850 70 20 B3 40 74 00 4D 04
                                                  02 03 72 30 A7 3F 10 02
              0C 00 1F 00 0C 08 6E 10
0013F860
                                                  DE 40 00 00 0A 00 0F
                                                                                 ពព
              91 00 06 07 28 FD 00 00
0013F870
                                                  08
                                                      00
                                                           02
                                                               00
                                                                   03
                                                                        00
                                                                            00
                                                                                 00
0013F880
                               3B 00 00 00
                                                  62 02 1E 17 38 02 12 00
                           00
              AF
                  87
              1B 03 2F 36 00 00 12 24
                                                  23 44 9A 08 12 05 4D 06
0013F890
0013F8A0
              04 05 12 15 4D 07 04 05
                                                  72
                                                      30 A7
                                                               3F
                                                                   32
                                                                        04 BE
                                                                                 00
0013F8B0
              12 72 12 63 6E 30 F1 3F
                                                  26 03 0A 00 14 02 50 00
                                                                                       ...
              0C 7F 6E 20 F4 3F 26 00
                                                  0C 01 1F
                                                               01 9B 07 22 02
0013F8C0
0013F8D0
              15 08 70 10 0D 41 02 00
                                                  1B 03 6E 44 00 00 6E 20
   AppCompatDelegateImpIV23_wrapWindowCaliback@L
                                                                                                                                  # CODE XREF:
                                                                 CODE:0013F806 locret:
  MainActivity_init_@V
                                                                 CODE:0013F806
                                                                                                     .line 17
  MainActivity_init_@VLL
                                                                 CODE: 0013F806
                                                                                                     return
  MainActivity access$super@LLLL
                                                                 CODE: 0013E808
  MainActivity_Add@III
MainActivity_Sub@III
                                                                 CODE:0013F808
                                                                 CODE:0013F808 loc_13F808:
                                                                                                                                  # CODE XREF:
  MainActivity_onClick@VL
                                                                                                     add-int
  MainActivity_onCreate@VL
                                                                 CODE:0013F80C
                                                                                                     goto
                                                                                                                                            locr
  DrawableCompat$LollipopDrawableImpl init @V
                                                                 CODE:0013F80C Method End
  DrawableCompat$LollipopDrawableImpl_applyTheme(
                                                                 CODE:0013F80C
  DrawableCompat$LollipopDrawableImpl_canApplyThe
                                                                 CODE: 0013F80E
                                                                                                     .byte 0, 0
  Drawable Compat \\ \$ Lollip op Drawable \\ Impl\_get Color \\ Filte
                                                                 CODE:0013F810 # =====
  DrawableCompat$LollipopDrawableImpl_inflate@VLLLI
                                                                 CODE:0013F810 # Method 16370 (0x3ff2)
  DrawableCompat$LollipopDrawableImpl_setHotspot@ +
                                                                 0013F808 0013F808: MainActivity_Add@III:loc_13F808 (Synchronized with Hex Vi
ine 11081 of 11231
加函数对应的指令
              70 20 B3 40 64 00 4D 04
0013F7D8
                                                   82 83 12 23 22 84 6
0013F7E8
               70 20 B3 40 74 00 4D 04
                                                   02 03 72 30 A7 3F 1
 0013F7F8
               OC 00 1F 00 OC 08 6E 10
                                                   DE
                                                        40 00 00 0A
0013F808
               90 00 06 07 28 FD 00 00
                                                   08
                                                       00 03 00 03
                                                                         00
0013F818
               A1 A7 21 00 2B 00 00 00
                                                   62 00 1E 17 38 00 2
 0013F828
               1B 01 44 17
                                00
                                    00 12 32
                                                   23 22 9A 08
                                                                     12
                                                                         03 4
0013F838
               02 03 12 13 22 04 03 08
                                                   70 20 B3 40 64 00 4
 0013F848
               02 03 12 23 22 04 03 08
                                                   70 20 R3 40 74 00 4
0013F858
               02 03 72 30 A7 3F 10 02
                                                   0C 00 1F 00 0C 08 6
0013F868
               DE 40 00 00 0A 00 0F 00
                                                   91 00 06 07 28 FD €
```

根据函数偏移,在内存中计算函数实际地址 A8A83028+0013F808=A8BC2830

G跳转则内存地址

```
A8BC2828
          DE 40
                   00
                      ពព
                          .0..
           0A 00
A8BC282C
                   ΩF
                      ពព
A8BC2830
          90
              00
                   06 07
A8BC2834
           28
              FD
                   00
                      00
                          (...
A8BC2838
           08 00
                   03 00
                          ----
A8BC283C
           03 00
                   00 00
A8BC2840
          A1
              A7
                   21
                      00
                          ....
A8BC2844
          2B 00
                   00
                      00
                          +...
          62 88
A8BC2848
                   1E 17
                          b . . .
A8BC284C
          38 00
                   26
                      00
                          8.8.
A8BC2850
          1B 01
                   44 17
                          ..D.
A8BC2854
          00 00
                  12 32
                          ...2
                          #"..
A8BC2858
          23 22
                  9A
                      08
```

```
A8BC282C
          00 A0
                 OF 00
                        . . . .
          91 86
                 06 07
A8BC2830
A8BC2834
          28 FD
                 00 00
A8BC2838
          08 00
                 03 00
A8BC283C
          03 00
                 00 00
A8BC2840 A1 A7
                 21 00
A8BC2844 2B 00
                 00 00
A8BC2848 62 00
                 1E 17
```

//加法变成可减法



成功!

下边dump下来

```
IDA - C:\Users\LAIvvEiv~1\AppData\Local\Temp\Iday9707.idb (app_process) - kunning
<u>File Edit Jump Search View Debugger Options W</u>indows Help
    New instance
<u>Open...</u>
    Load file
    Produce file
Script file...
                                                                    Alt+F7
Script command...
                                                                    Shift+F2
                                                                    Ctrl+W
    Save
    Save as...
Take database snapsho<u>t</u>...
                                                                    Ctrl+Shift+W
A8A83824 C7 B2 D2 6D
A8A83028
          64 65
                 78 OA
A8A8302C 30 33
                 35 00
                         035.
A8A83030 AC 26
                 2E 48
                         .&.H
A8A83034
         3E 56
                 6D 52
                         >UmR
A8A83038 10 DO
                 6A 4E
                         ..jN
                         ~B..
A8A8303C 7E 42
                 BF ØD
A8A83040 BC DD
                 E8 AF
A8A83044 66 E6
                 26 99
A8A83048
          94 1A
                         ..&.
         70 00
A8A8304C
                 00 00
A8A83050 78 56
                 34 12
A8A83054
          00 00
                 00 00
A8A83058 00 00 00 00
先取出起始地址,还有文件大小4个字节
起始地址: A8A83028
大小: 261A94
static main(void)
  auto fp, begin, end, dexbyte;
  fp = fopen("d:\\dump.dex", "wb");
  begin = 0xA8A83028; //基址
  end = begin + 0x261a94; //大小
  for ( dexbyte = begin; dexbyte < end;
                                          dexbyte ++ )
     fputc(Byte(dexbyte), fp);
```

```
in = 0xA8A83028; //基址
= begin + 0x261a94; //大小
( dexbyte = begin; dexbyte < end; dexbyte ++ )
fputc(Byte(dexbyte), fp);

Please wait...

Running IDC script

Cancel
```

• dump之后可以使用最新版的baksmali反编译dex文件