sekkr1 / **android_gdb.md**

Created 3 years ago

☆ Star

<> **Code** -o-Revisions 2 ☆Stars 7 Forks 4

Attaching GDB to Android apps' native libraries

android_gdb.md

How to GDB android native libraries

[1] Install NDK from android studio

[2] Push appropriate gdb-server to phone

```
adb push ~/android-sdk-linux/ndk-bundle/prebuilt/android-<arch>/gdbserver/gdbserver /data/local/tmp
adb shell "chmod 777 /data/local/tmp/gdbserver"
adb shell "ls -l /data/local/tmp/gdbserver"
```

[4] Forward ports

`adb forward tcp:1337 tcp:1337`

[5] Copy libraries for symbols

```
mkdir -p ~/dbgtmp/
adb pull /system/lib ~/dbgtmp/
adb pull /data/data/<app package>/<lib folder>/* ~/dbgtmp
```

[6] Start application in debug mode

```
am set-debug-app -w --persistent <app name>
am start -n <app name>/<main activity>
```

[7] Attach debugger

PID=``adb shell ps | grep instagram | grep -v : | awk '{print $2}'``; CMD="/data/local/tmp/gdbserver :1337 --attach ${PID}"; adb shell su -c "${CMD}"

[8] Start and connect gdb

```
~/android-sdk-linux/ndk-bundle/prebuilt/linux-x86_64/bin/gdb
set solib-search-path ~/dbgtmp/lib
target remote :1337
```

Notes

To get module base address

Either in GDB

```
info file <module name>l
set $base = <module start address gotten from last command>
```

Or in adb shell PID=``adb shell ps | grep instagram | grep -v : | awk '{print $2}'``; adb shell su -c cat /proc/${PID}/maps | grep <app name>

GDB constantly stops on irrelevant signals

handle <signal name> noprint nostop

It is recommended you put your gdb configs in ~/gdbinit, example:

```
define instagram
        target remote :1337
        set solib-search-path ~/dbgtmp/lib
        handle SIGSEGV noprint nostop
        handle SIG33 noprint nostop
        handle SIGILL noprint nostop
        printf "Signal handlers on"
end
```

Stop on load of shared libraries

`set stop-on-solib-events 1`