Android Mobile Pentest 101

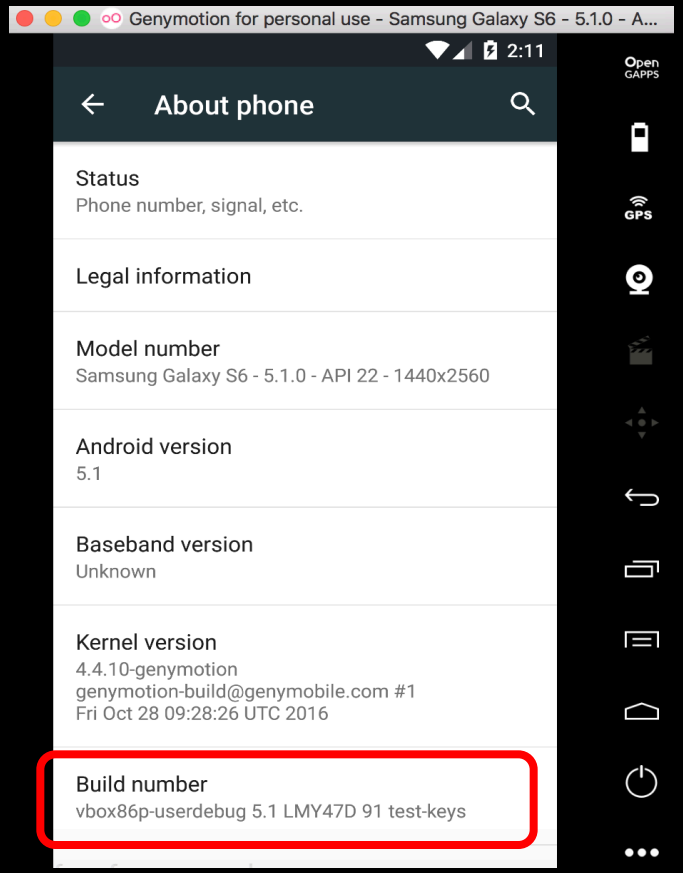
Bài 2 – Android Tool

Mục tiêu: xài được adb (android debug bridge)

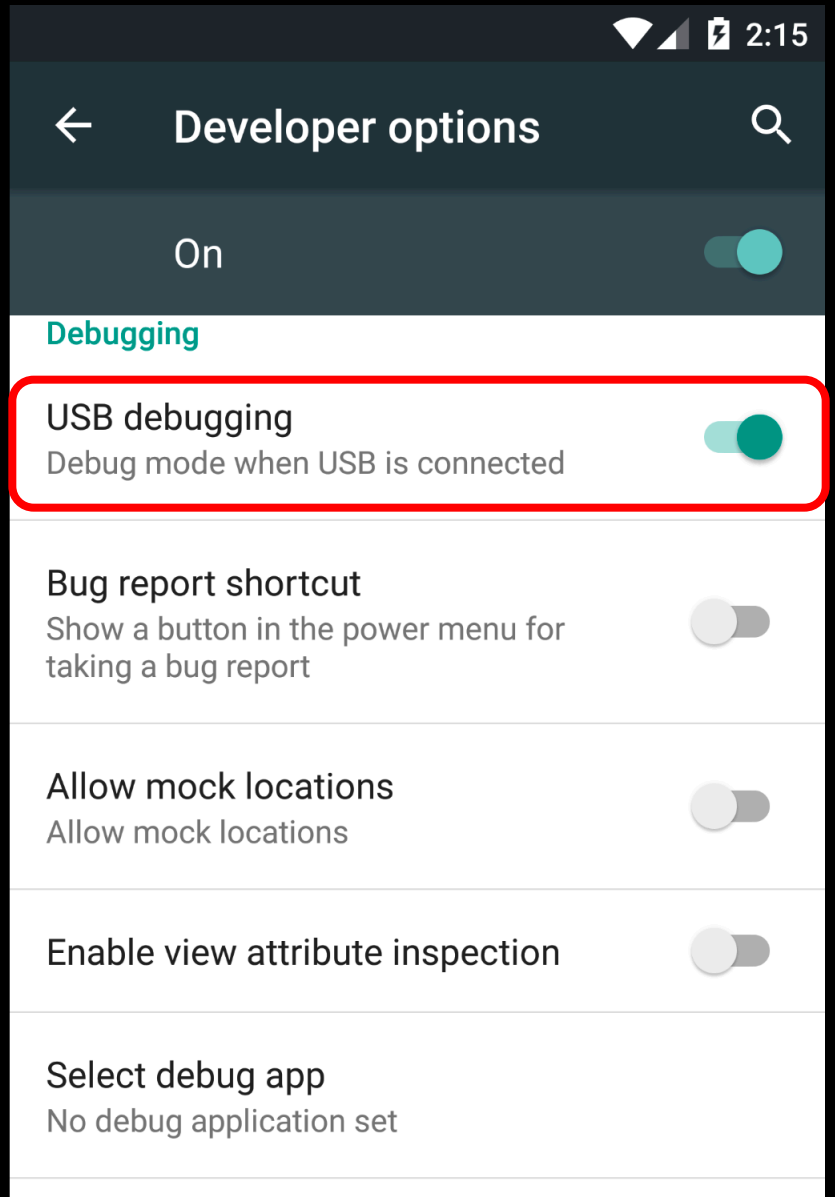
- Đầu tiên bạn cần phải biết làm thế nào để cài 1 tập tin apk vào điện thoại
- Tải file apk tại đường dẫn sau

https://github.com/dineshshetty/Android-InsecureBankv2/blob/master/InsecureBankv2.apk

- Trên điện thoại ảo vừa tạo, chọn Settings -> About Phone -> bấm 6 đến 12 lần vào trường Build Number để bật chế độ developer



- Về lại Settings, bạn sẽ thấy trường Developer options xuất hiện, chọn nó
- Ở trong đó thì bật USB Debugging lên, chức này cho phép ta tương tác điện thoại ảo với máy thật



- Bây giờ bạn đã đủ điều kiện để cài 1 file apk bằng adb
- Genymotion sử dụng adb riêng biệt, do đó chúng ta phải vào thư mục của genymotion và tìm nó

Trên máy mac nó nằm ở "<Chuột phải vào biểu tượng Genymotion -> Show Packages Contents>/Contents/MacOS/tools/adb"

Trên windows nó nằm ở "C:\Program Files\Genymobile\Genymotion\tools\adb.exe"

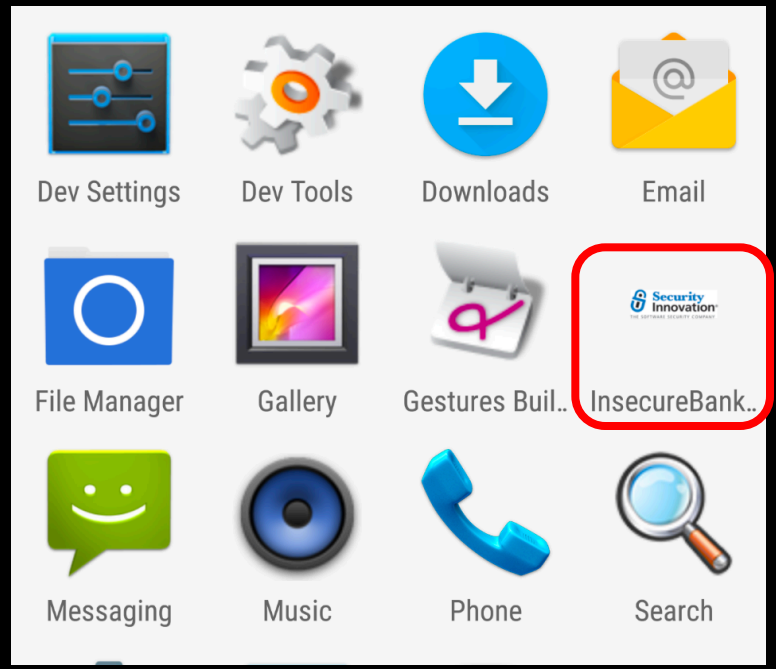
192.168.56.101 là địa chỉ ip của điện thoại ảo, và chúng ta sẽ tương tác từ máy thật với nó qua cổng 5555

- Cài file apk vào điện thoại ảo bằng câu lệnh:

adb install /path/to/apkfile

```
1. tsug0d@Nguyens-MBP: ~/Desktop/mobile/tools (zsh)
 ~/Desktop/mobile/tools/ ./adb install InsecureBankv2.apk
InsecureBankv2.apk: 1 file pushed. 73.0 MB/s (3632378 bytes in 0.047s)
        pkg: /data/local/tmp/InsecureBankv2.apk
Success
```

- Xem trên điện thoại, ta thấy file đã cài đặt thành công



- Để vào command-line shell của điện thoại, gõ lệnh:

adb shell

```
 ~/Desktop/mobile/tools/ ./adb shell
root@vbox86p:/ # whoami
root
root@vbox86p:/ # uname -a
Linux localhost 4.4.10-genymotion #1 SMP PREEMPT Fri Oct 28 09:28:26 UTC 2016 x86_64 GNU/Linux
```

- Để xem log, gõ lệnh:

adb logcat

```
eued tasks = 0, completed tasks = 1]
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.JobSchedulerEngine$PhoneskyJobSchedulerJobService.onStartJo
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.v.a(39): Scheduling fallback in 43199999 (absolute: 8127723
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.v.a(39): Scheduling fallback in 64799998 (absolute: 1028772
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.JobSchedulerEngine$PhoneskyJobSchedulerJobService.onStartJo
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.v.a(39): Scheduling fallback in 43199999 (absolute: 8127724
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.v.a(39): Scheduling fallback in 64799999 (absolute: 1028772
W/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.JobSchedulerEngine$PhoneskyJobSchedulerJobService.onStartJo
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.ac.handleMessage(16): DeviceState: DeviceState{currentTime=
rue, netUnmetered=true}
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.ba.a(64): Jobs in database: 1-1337 12-1
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.x.a(58): Running job: 12-1
I/Finsky  ( 9894): [1] com.google.android.finsky.contentsync.ContentSyncJob.a(28): ContentSyncJob started
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.x.a(99): RunningQueue size: 1, PendingQueue size: 0
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.x.a(108): Running queue: 12-1
I/Finsky  ( 9894): [299] com.google.android.finsky.m.c.a(20): Completed 0 account content syncs with 0 successful.
I/Finsky  ( 9894): [1] com.google.android.finsky.contentsync.ContentSyncJob.a(26): Installation state replication succ
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.ax.b(8): jobFinished: 12-1. TimeElapsed: 2ms
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.x.a(132): Job 12-1 finished
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.x.a(99): RunningQueue size: 0, PendingQueue size: 0
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.ac.handleMessage(41): Executor finished
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.ba.a(64): Jobs in database: 1-1337
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.g.a(68): ConstraintMapping: 1-1337,  -> L: 43448120ms, D: 1
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.JobSchedulerEngine.a(93): Scheduling job Id: 9000, L: 43448
I/Finsky  ( 9894): [1] com.google.android.finsky.scheduler.JobSchedulerEngine.a(93): Scheduling job Id: 9002, L: 43448
I/Finsky  ( 9894): [288] com.google.android.finsky.bn.ab.run(5): Stats for Executor: BlockingExecutor com.google.andro
d tasks = 0, completed tasks = 0]
I/Finsky  ( 9894): [288] com.google.android.finsky.bn.ab.run(5): Stats for Executor: LightweightExecutor com.google.an
eued tasks = 0, completed tasks = 1]
I/Finsky  (10034): [302] com.google.android.finsky.bn.ab.run(5): Stats for Executor: BlockingExecutor com.google.andro
d tasks = 0, completed tasks = 0]
```

- Để tải lên một file từ máy thật đến điện thoại ảo, gõ lệnh:

adb push </path/to/file/pc> </path/to/file/device>

```
 ~/Desktop/mobile/tools/ echo "test" > /tmp/xxx
 ~/Desktop/mobile/tools/ ./adb push /tmp/xxx /tmp/file_on_device
/tmp/xxx: 1 file pushed. 0.0 MB/s (5 bytes in 0.003s)
 ~/Desktop/mobile/tools/ ./adb shell
root@vbox86p:/ # cat /tmp/file_on_device
test
```

- Để tải một file từ điện thoại ảo xuống về máy thật, gõ lệnh:

adb pull </path/to/file/device> </path/to/file/pc>

```
root@vbox86p:/ # echo "from device" > /tmp/gg
root@vbox86p:/ # exit
 ~/Desktop/mobile/tools/ ./adb pull /tmp/gg /tmp/pc-file
/tmp/gg: 1 file pulled. 0.0 MB/s (12 bytes in 0.001s)
 ~/Desktop/mobile/tools/ cat /tmp/pc-file
from device
 ~/Desktop/mobile/tools/
```