# Android Mobile Pentest 101

© tsug0d, September 2018

Lecture 2 – Android Tool

Goal: Got a knowledge about android debug bridge

- First, you need to know how to install an apk into our virtual device
- Download the test apk here:
https://github.com/dineshshetty/Android-InsecureBankv2/blob/master/InsecureBankv2.apk

- In our virtual phone, go to Settings -> About Phone -> do from 6 to 12 clicks on Build Number to become developer
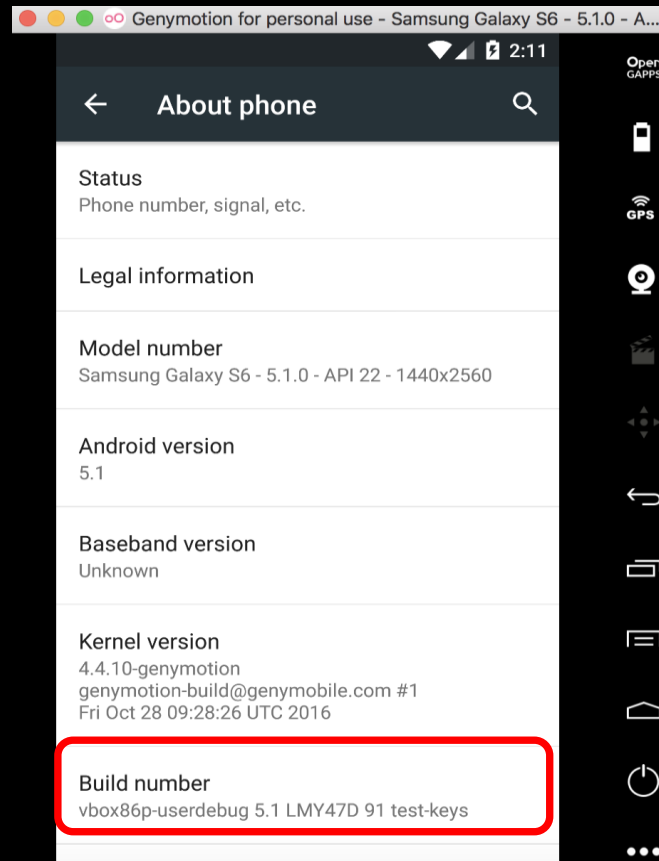
- Go back to Settings, now the Developer options is appear, click it
- In Developer tab, enable USB Debugging option, it allows the phone interact with our pc
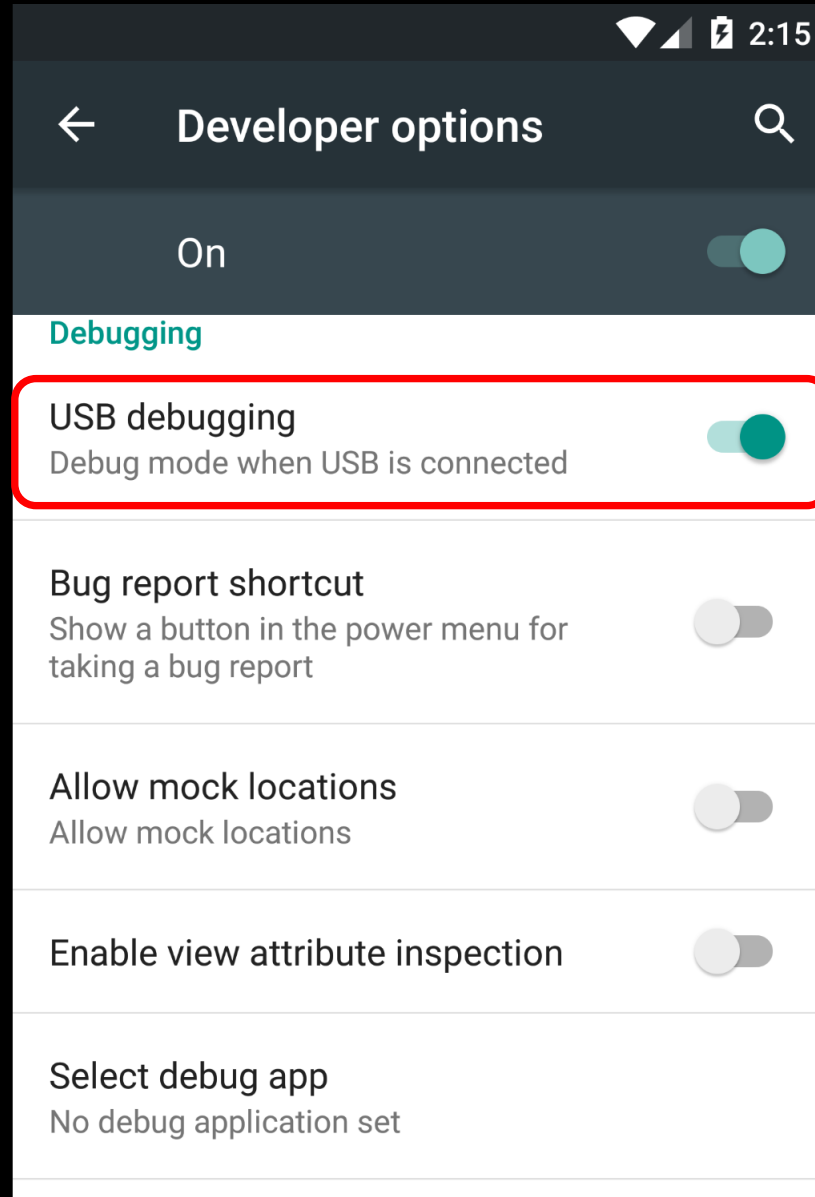
- Now you are ready to install your very first android program via adb
- Genymotion use specify adb, so go to its folder and find it

On mac its located in "<Right Click on Genymotion -> Show Packages Contents>/Contents/MacOS/tools/adb"

On windows its located in "C:\Program Files\Genymobile\Genymotion\tools\adb.exe"

- Check if it works perfectly:

```
1. tsug0d@Nguyens-MBP: ~/Desktop/mobile/tools (zsh)

 ~/Desktop/mobile/tools/ ./adb devices
List of devices attached
192.168.56.101:5555     device

 ~/Desktop/mobile/tools/ █
```

192.168.56.101 is the ip address of our virtual phone, and we will interact with it via port 5555

- Install the apk into our phone via command:
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
```

- Go to the phone and check if it is installed
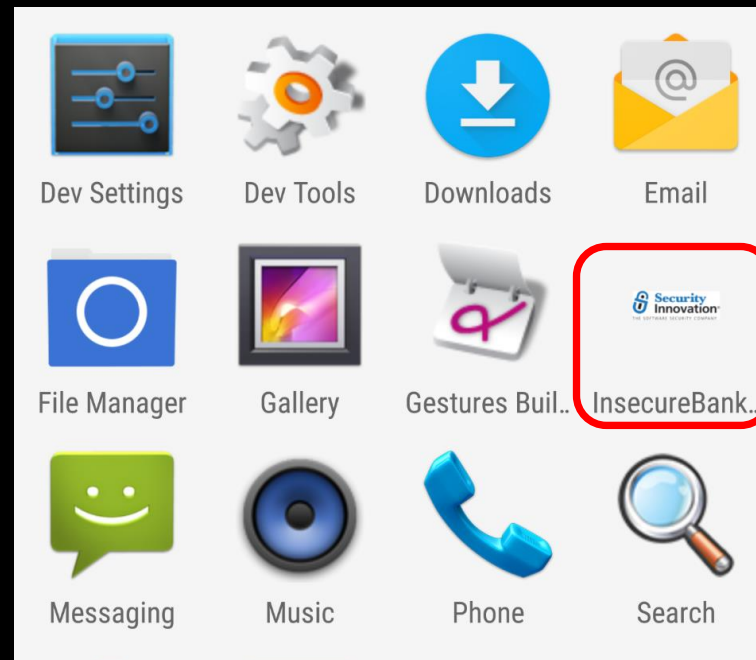
- Important! To use the app InsecureBankv2, you need to start a server, because mobile app is just a client app, it will send request to the server outside ☺

- Get this folder:
https://github.com/dineshshetty/Android-InsecureBankv2/tree/master/AndroLabServer

- Then:
- cd AndroLabServer
- pip install -r requirements.txt
- python app.py

- Your server will be started at <ip-address>:<port8888> by default
- Turn on app InscureBankv2 and fill-in the server info ☺, done

- To access device shell, type command:

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
```

- To view log of the phone, type command:

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]
```

- To push file to device, type command:

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
```

- To pull file from device, type command:

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/ 
```