Android Mobile Pentest 101

Bài 8 – Các công cụ hỗ trợ

Mục tiêu: Tăng tốc quá trình pentest

Why?

- Giả sử chúng ta quá gà, hoặc cái app quá khó, không reverse được, không patch được, không hook được nốt, etc... Thế là bỏ cuộc hử?
- Đừng lo lắng, có thể công cụ sẽ giúp được bạn. Mình cũng thường xài công cụ trước, nếu thất bại mới làm tay ☺
- Ở bài này mình giới thiệu các tool dùng để bypass root detection, emulator detection and ssl pinning

Root Detection Bypass

- Để bypass root detection, Chúng ta sẽ sử dụng RootCloak
- Đây là 1 module của Xposed Framework
- Bằng nhiều cách khác nhau, nó sẽ làm app không thấy được root trên điện thoại
- Cụ thể là ẩn đi su binary, superuser/supersu apks, processes chạy bởi root, adb, vv.

Root Detection Bypass -> Install

- Vì nó là module của Xposed Framework, nên chúng ta sẽ cài Xposed trước
- Cài bằng MobSF script:

https://github.com/MobSF/Mobile-Security-Framework-MobSF/blob/master/scripts/mobsfy.py

- Gõ lệnh:

python3 mobsfy.py -i 192.168.56.101:5555 -t 1

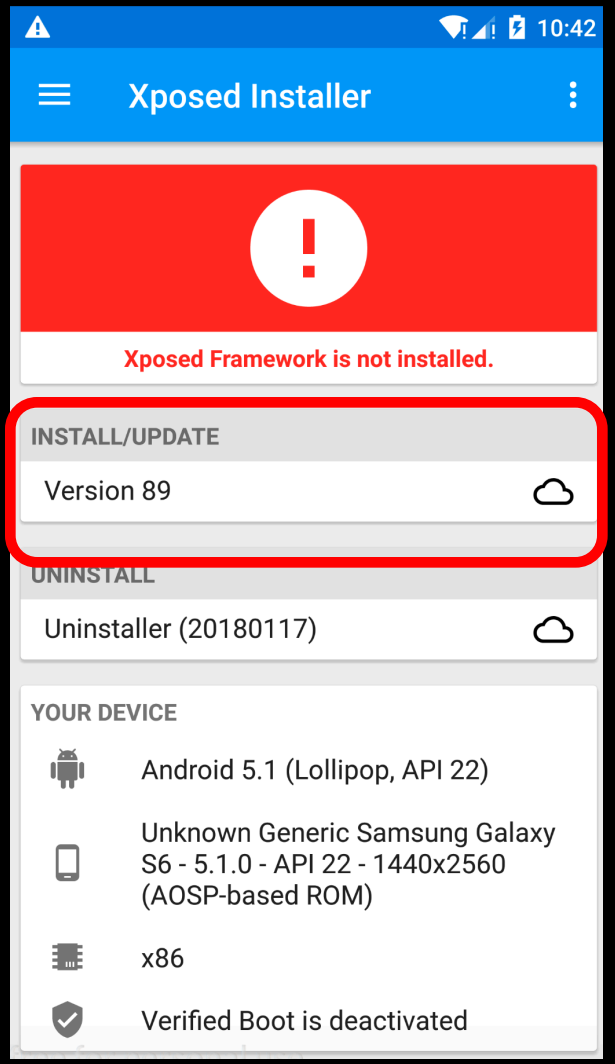
Địa chỉ ip trong lệnh là của điện thoại ảo, giá trị của –t bằng 1 để chỉ định nó là ảo, nếu 2 là thiết bị thật

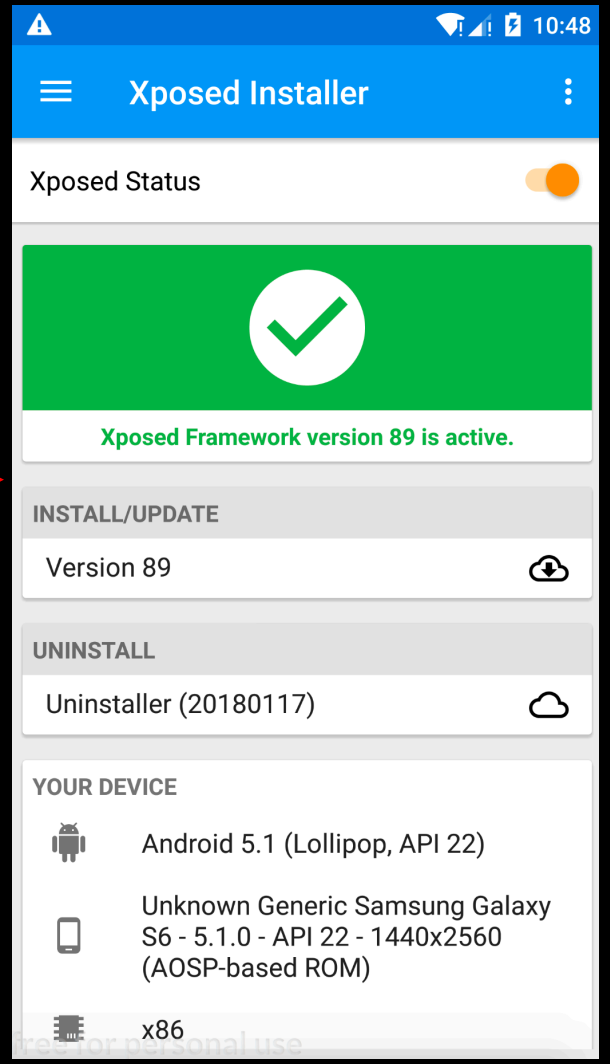
```
[INFO] Executing Command - /Users/tsug0d/Desktop/mobile/tools/Mobile-Security-Framework-MobSF/scripts/../DynamicAnalyzer/tools/adb/mac/adb connect 192.168.56
.101:5555
adb server version (40) doesn't match this client (39); killing...
adb E 09-25 09:35:02  4717 409269 usb_osx.cpp:152] Unable to create an interface plug-in (e00002be)
error: could not install *smartsocket* listener: Address already in use
ADB server didn't ACK
* failed to start daemon *
error: cannot connect to daemon
```

- Không được! Bởi vì chúng ta đang xài genymotion, ta phải sử dụng geny adb, đổi cái adb trong đường dẫn với genymotion adb là xong

Root Detection Bypass -> Install

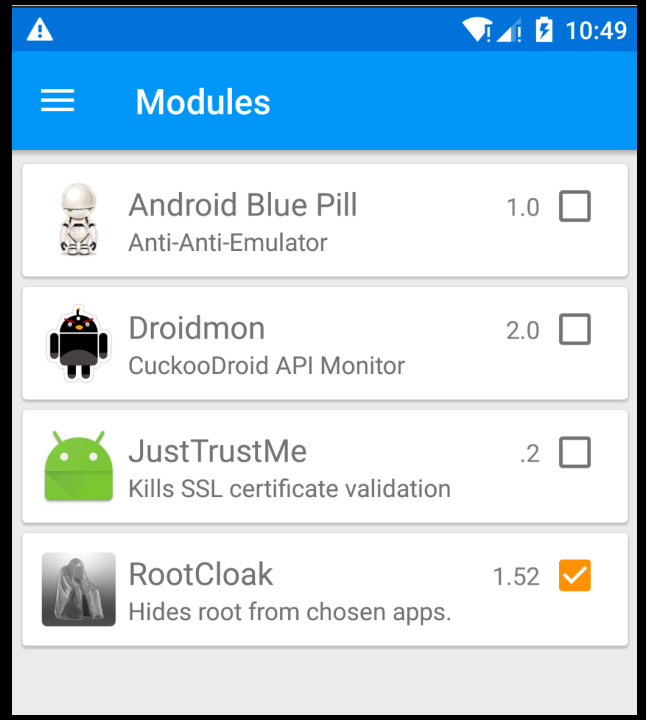
- Chạy lại lệnh, Xposed xuất hiện trên phone, nhưng vẫn chưa được cài, ta phải click vào chỗ install





Root Detection Bypass -> Install

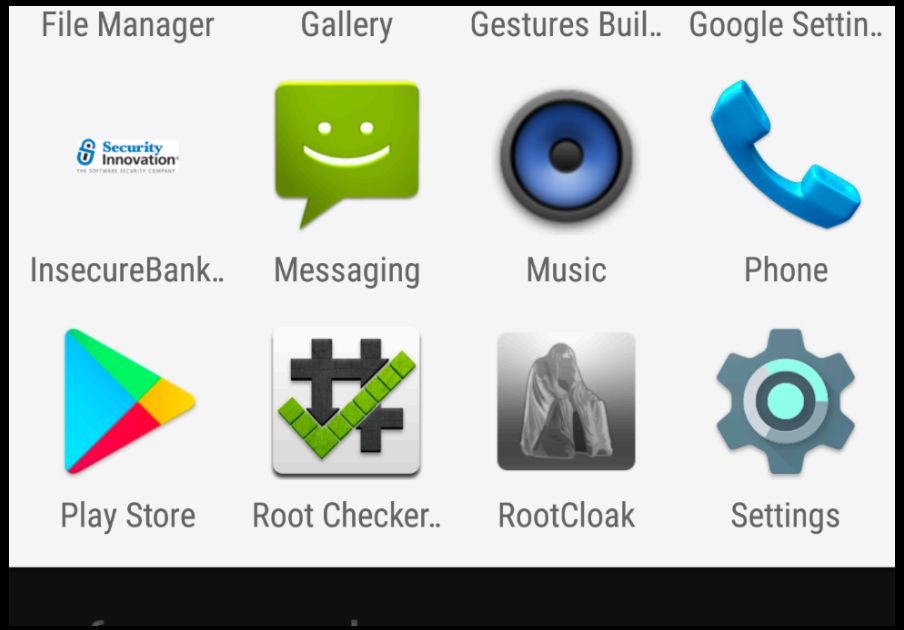
- Bây giờ đi tới Modules task của Xposed và chọn RootCloak



- Khởi động lại

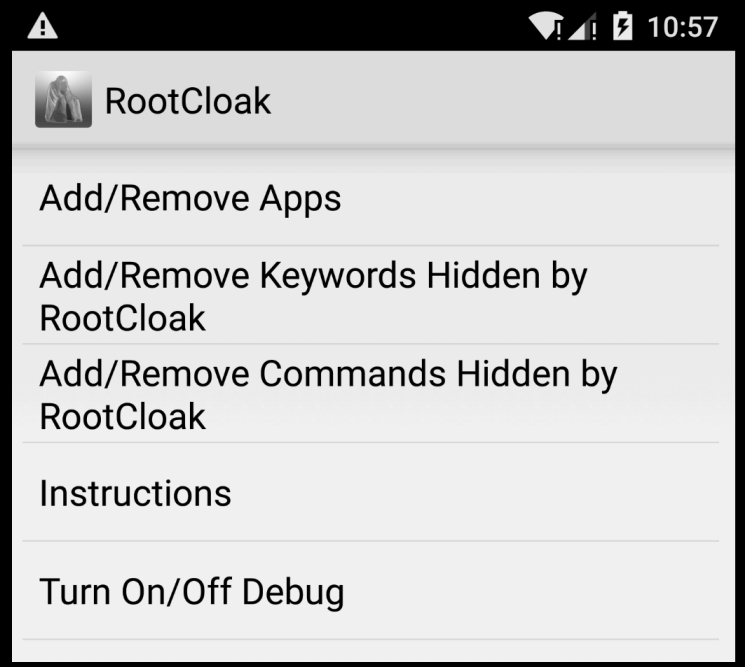
Root Detection Bypass -> Install

- RootCloak đã xuất hiện ☺



Root Detection Bypass -> Using

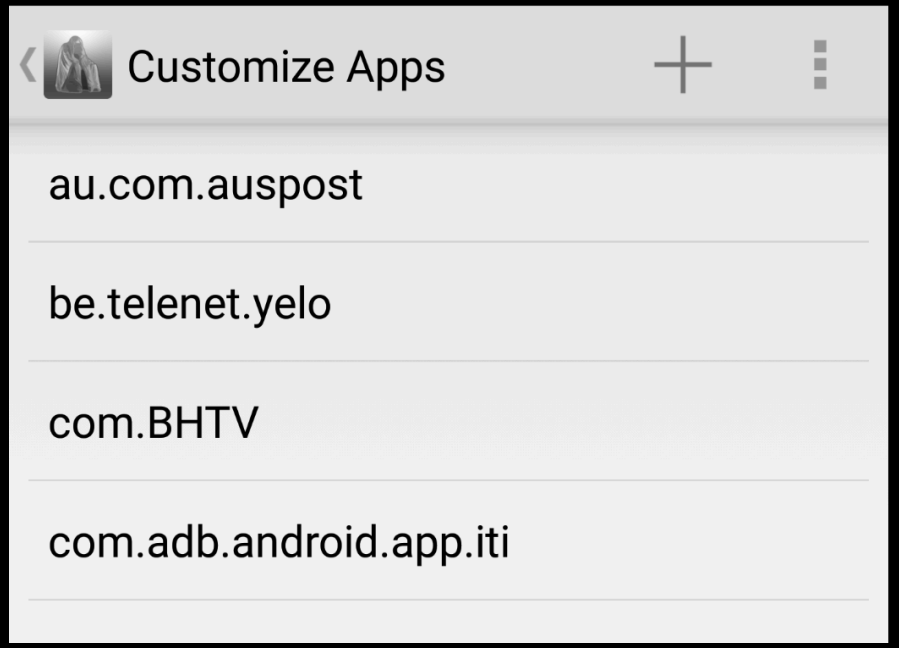
- Mở RootCloak lên, nó sẽ trông như vậy



- Chọn Add/Remove Apps

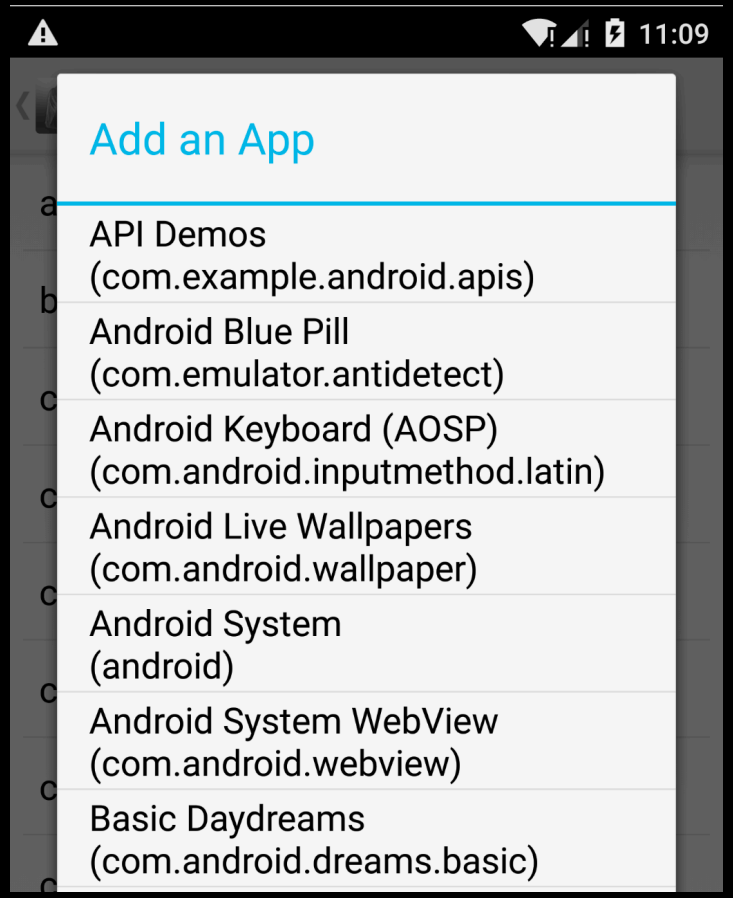
Root Detection Bypass -> Using

- Bấm vào dấu cộng



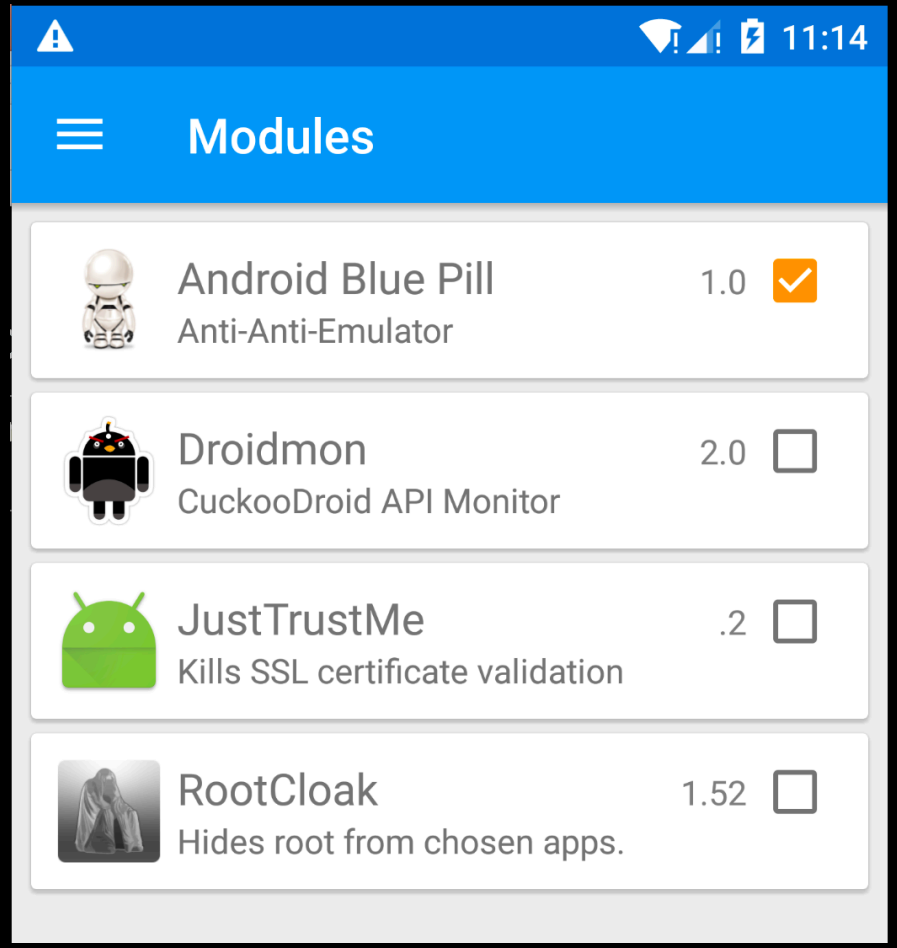
Root Detection Bypass -> Using

- Chọn app cần hide root, vậy là xong



Emulator Detection Bypass

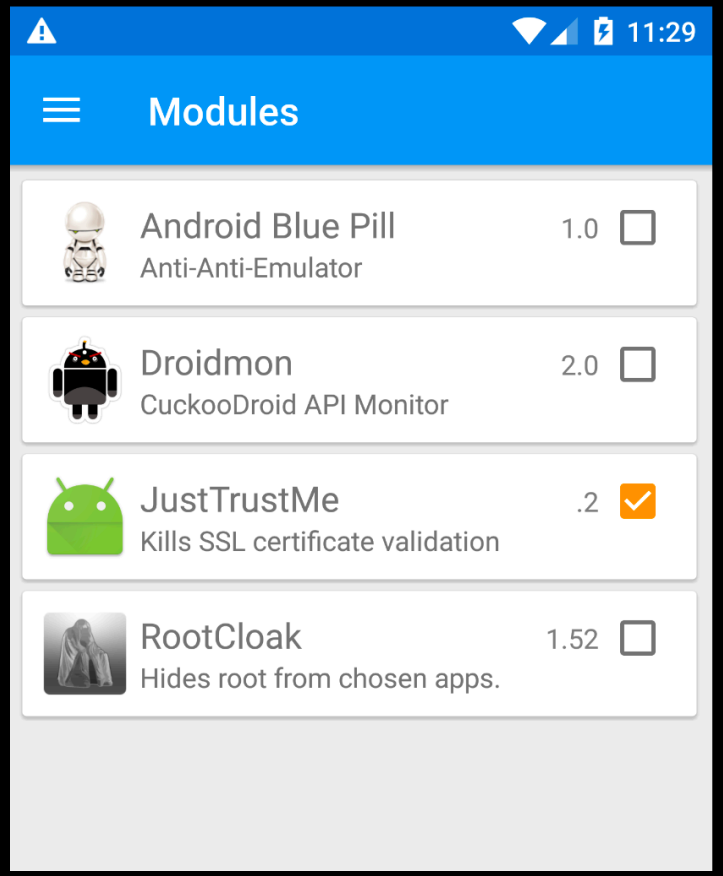
- Tương tự như bypass root, Ta chọn Android Blue Pill trong Xposed



- Khởi động lại, done (Giới thiệu thôi, chứ thường mình không xài được cái này ☺)

SSL Pinning Bypass -> JustTrustMe

- Ở Phần này, mình sẽ nói về 2 công cụ mình luôn xài, đầu tiên là JustTrustMe thuộc Xposed Modules



- Tick on it, reboot, done
- Cái này cũng cũ rồi, lúc được lúc không, nên mình xài thêm cái nữa

SSL Pinning Bypass -> Objection

- Nhớ slide cuối của bài 6 không? Chúng ta sẽ sử dụng Objection - a runtime mobile exploration toolkit, powered by Frida, để bypass ssl pinning
- Objection được tạo ra để đánh giá bảo mật các ứng dụng di động mà không cần jailbroken hay root

Note: Objection không hỗ trợ jailbreak / root bypass.

SSL Pinning Bypass -> Objection

- Để cài đặt, gõ lệnh:

pip3 install objection

- Kiểm tra thử coi:

```
 ~/Desktop/mobile/tools/objection/ objection
Usage: objection [OPTIONS] COMMAND [ARGS]...

           _     _           _   _
 ___ ___ |_|___ ___| |_|_|___ ___
| . | . | | | -_|  _|  _| | . |   |
|___|___|_| |___|___|_| |_|___|_|_|
        |___|(object)inject(ion)

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

  By default, communications will happen over USB, unless the --network
  option is provided.
```

SSL Pinning Bypass -> Objection

- Để sử dụng Objection, cần 2 thứ:

1. Objection installed
2. File APK của app được patch bởi objection được cài trên điện thoại ảo, và debug được thông qua usb

Cái 1 chúng ta đã có, nên giờ tạo file apk patched, gõ lệnh:

objection patchapk --source InsecureBankv2.apk

(More about this: https://github.com/sensepost/objection/wiki/Patching-Android-Applications)

- Kết quả:

```
 ~/Desktop/mobile/tools/objection/ objection patchapk --source InsecureBankv2.apk
No architecture specified. Determining it using `adb`...
Detected target device architecture as: x86
Using latest Github gadget version: 12.2.5
Patcher will be using Gadget version: 12.2.5
Unpacking InsecureBankv2.apk
App already has android.permission.INTERNET
Reading smali from: /var/folders/h1/rxkqmv9d69vg7j1cw8k1d13m0000gn/T/tmp8vw27ag0.apktemp/smali/com/android/insecurebankv2/LoginActivity.smali
Injecting loadLibrary call at line: 24
Writing patched smali back to: /var/folders/h1/rxkqmv9d69vg7j1cw8k1d13m0000gn/T/tmp8vw27ag0.apktemp/smali/com/android/insecurebankv2/LoginActivity.smali
Creating library path: /var/folders/h1/rxkqmv9d69vg7j1cw8k1d13m0000gn/T/tmp8vw27ag0.apktemp/lib/x86
Copying Frida gadget to libs path...
Rebuilding the APK with the frida-gadget loaded...
Built new APK with injected loadLibrary and frida-gadget
Signing new APK.
Signed the new APK
Performing zipalign
Zipalign completed
Copying final apk from /var/folders/h1/rxkqmv9d69vg7j1cw8k1d13m0000gn/T/tmp8vw27ag0.apktemp.aligned.objection.apk to InsecureBankv2.objection.apk in current
directory...
Cleaning up temp files...
```

SSL Pinning Bypass -> Objection

- Bây giờ chúng ta cài file apk vừa patch

```
 ~/Desktop/mobile/tools/objection/ adb install InsecureBankv2.objection.apk
InsecureBankv2.objection.apk: 1 file pushed. 87.4 MB/s (10230246 bytes in 0.112s)
WARNING: linker: libhoudini.so has text relocations. This is wasting memory and prevents security hardening. Please fix.
        pkg: /data/local/tmp/InsecureBankv2.objection.apk
Success
```

- Chạy app vừa cài trên điện thoại, sau đó gõ lệnh:

```
objection --gadget "com.android.InsecureBankv2" explore
```

```
     _     _         _   _
 ___| |_  |_|___ ___| |_|_|___ ___
| . | . | | | -_|  _|  _| | . |   |
|___|___|_| |___|___|_| |_|___|_|_|
        |___|(object)inject(ion) v1.4.3

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
com.android.insecurebankv2 on (google: 5.1) [usb] #
```

SSL Pinning Bypass -> Objection

- Với Objection chúng ta có thể thu thập thông tin về app, ví dụ lệnh env sẽ trả về vị trí của các thư mục Files, Caches và nhiều thư mục khác:

```
com.android.insecurebankv2 on (google: 5.1) [usb] # env

Name                  Path
--------------------  ------------------------------------------------------------
filesDirectory        /data/data/com.android.insecurebankv2/files
cacheDirectory        /data/data/com.android.insecurebankv2/cache
externalCacheDirectory  /storage/emulated/0/Android/data/com.android.insecurebankv2/cache
codeCacheDirectory    /data/data/com.android.insecurebankv2/code_cache
obbDir                /storage/emulated/0/Android/obb/com.android.insecurebankv2
packageCodePath       /data/app/com.android.insecurebankv2-1/base.apk
```

SSL Pinning Bypass -> Objection

- Hoặc liệt kê các Activities mà app có:

```
com.android.insecurebankv2 on (google: 5.1) [usb] # android hooking list activities
com.android.insecurebankv2.ChangePassword
com.android.insecurebankv2.DoLogin
com.android.insecurebankv2.DoTransfer
com.android.insecurebankv2.FilePrefActivity
com.android.insecurebankv2.LoginActivity
com.android.insecurebankv2.PostLogin
com.android.insecurebankv2.ViewStatement
com.android.insecurebankv2.WrongLogin
com.google.android.gms.ads.AdActivity
com.google.android.gms.ads.purchase.InAppPurchaseActivity

Found 10 classes
```

- Sử dụng activities liệt kê được, invoking arbitrary activities:

```
com.android.insecurebankv2 on (google: 5.1) [usb] # android intent launch_activity com.android.insecurebankv2.PostLogin
Launching Activity: com.android.insecurebankv2.PostLogin...
Launched: com.android.insecurebankv2.PostLogin
```

SSL Pinning Bypass -> Objection

- Lang man quá, trở về chủ đề chính, để bypass SSL Pinning sử dụng Objection, gõ lệnh (mặc dù app của chúng ta không có ssl pinning, ví dụ thôi ☺):

android sslpinning disable

```
com.android.insecurebankv2 on (google: 5.1) [usb] # android sslpinning disable
Job: ddd0adc5-872b-4f22-9c6f-84b1c0150a1a - Starting
[84b1c0150a1a] [android-ssl-pinning-bypass] Custom, Empty TrustManager ready
[84b1c0150a1a] [android-ssl-pinning-bypass] TrustManagerImpl
Job: ddd0adc5-872b-4f22-9c6f-84b1c0150a1a - Started
```

- Xong! Objection còn nhiều tính năng vui lắm, tìm hiểu thử nha ☺