

# BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 2: Memory Forensics

GVHD: Nghi Hoàng Khoa

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Võ Sỹ Minh	21521146	21521146@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	80%
3	Yêu cầu 3	80%
4	Yêu cầu 4	50%
5	Yêu cầu 5	100%
6	Yêu cầu 6	100%
7	Yêu cầu 7	80%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

---

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## 1. Phân tích tĩnh (Static Analysis)

Dùng MobSF phân tích tĩnh file InsecureBankv2.apk.

The screenshot displays the MobSF Static Analyzer interface. The left sidebar shows the navigation menu with 'Static Analyzer' selected. The main content area is divided into three sections: APP SCORES, FILE INFORMATION, and APP INFORMATION.

**APP SCORES:** Security Score 28/100, Trackers Detection 3/432. A MobSF Scorecard link is provided.

**FILE INFORMATION:** File Name: InsecureBankv2.apk, Size: 3.3MB, MD5: 5ee4829065640f9c936ac861d1650ffc, SHA1: 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98, SHA256: b18af2a0e44d7634bbcdf93664d9c78a2695e050393fcfb5e8b91f902d194a4.

**APP INFORMATION:** App Name: InsecureBankv2, Package Name: com.android.insecurebankv2, Main Activity: com.android.insecurebankv2.LoginActivity, Target SDK: 22, Min SDK: 15, Max SDK: 15, Android Version Name: 1.0, Android Version Code: 1.

Below these sections, there are four cards representing different app components: ACTIVITIES (10), SERVICES (0), RECEIVERS (2), and PROVIDERS (1). Each card has a 'View' button and an 'Exported' section showing the count of exported items (Activities: 4, Services: 0, Receivers: 1, Providers: 1).

The bottom section of the screenshot shows a table of permissions. The 'Permissions' tab is selected in the sidebar.

Permission	Level	Description	Action
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks. <a href="#">Show Files</a>
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets. <a href="#">Show Files</a>
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation. <a href="#">Show Files</a>
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens. <a href="#">Show Files</a>
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete	Allows an application to write to external storage. <a href="#">Show Files</a>

MANIFEST ANALYSIS				
HIGH 6		WARNING 7		INFO 0
				SUPPRESSED 0
NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 4.0.3-4.0.4, [minSdk=15]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.	
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.	
4	Activity (com.android.insecurebankv2.PostLogin) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be	

Có những Issue có mức độ cao ở đây, có khả năng rất cao thực hiện các hành vi độc hại

Tiếp tục với công cụ Bytecode-Viewer:

Xem file DoLogin.class

File View Settings Plugins

Files

ChangePassword\$Req

ChangePassword.class

CryptoClass.class

DoLogin\$RequestTask

DoLogin.class

DoTransfer\$1.class

DoTransfer\$2.class

DoTransfer\$RequestD

DoTransfer\$RequestD

DoTransfer\$RequestD

DoTransfer\$RequestD

DoTransfer.class

Quick file search (no file e

Exact Path

Match Case

Exact

Search

Search From: All Classes

Strings

Search String:

Exact

Search

Results

Work Space

resources.arsc x com/android/insecurebankv2/DoLogin.class

FernFlow Decompiler

package com.android.insecurebankv2;

import android.app.Activity;

import android.content.Intent;

import android.content.SharedPreferences;

import android.os.Bundle;

import android.preference.PreferenceManager;

import android.view.Menu;

import android.view.MenuItem;

import android.widget.Toast;

import java.io.BufferedReader;

public class DoLogin extends Activity {

public static final String MYPREFS = "mySharedReferences";

String password;

String protocol = "http://";

BufferedReader reader;

String rememberme\_password;

String rememberme\_username;

String responseString = null;

String result;

SharedPreferences serverDetails;

String serverip = "";

String serverport = "";

String superSecurePassword;

String username;

public void callPreferences() {

this.startActivity(new Intent(this, FilePrefActivity.class));

}

protected void onCreate(Bundle var1) {

super.onCreate(var1);

this setContentView(2130968602);

this.finish();

this.serverDetails = PreferenceManager.getDefaultSharedPreferences(this);

this.serverip = this.serverDetails.getString("serverip", (String)null);

this.serverport = this.serverDetails.getString("serverport", (String)null);

if (this.serverip != null && this.serverport != null) {

Intent var2 = this.getIntent();

this.username = var2.getStringExtra("passed\_username");

this.password = var2.getStringExtra("passed\_password");

(new RequestTask(this)).execute(new String[] { "username" });

} else {

Bytecode Disassembler

public class com/android/insecurebankv2/DoLogin extends android/app/Activity {

<ClassVersion=50>

public static final java.lang.String MYPREFS = "mySharedReferences";

java.lang.String password;

java.lang.String protocol;

java.io.BufferedReader reader;

java.lang.String rememberme\_password;

java.lang.String rememberme\_username;

java.lang.String responseString;

java.lang.String result;

android.content.SharedPreferences serverDetails;

java.lang.String serverip;

java.lang.String serverport;

java.lang.String superSecurePassword;

java.lang.String username;

public DoLogin() { // <init> //()

aload 0 // reference to self

invokevirtual android/app/Activity.<init>()V

aload 0 // reference to self

aconst null

putfield com/android/insecurebankv2/DoLogin.responseString:java.lang.String

aload 0 // reference to self

ldc "" (java.lang.String)

putfield com/android/insecurebankv2/DoLogin.serverip:java.lang.String

aload 0 // reference to self

ldc "" (java.lang.String)

putfield com/android/insecurebankv2/DoLogin.serverport:java.lang.String

aload 0 // reference to self

ldc "http://" (java.lang.String)

putfield com/android/insecurebankv2/DoLogin.protocol:java.lang.String

return

}

public void callPreferences() { //()

aload 0 // reference to self

new android/content/Intent

dup

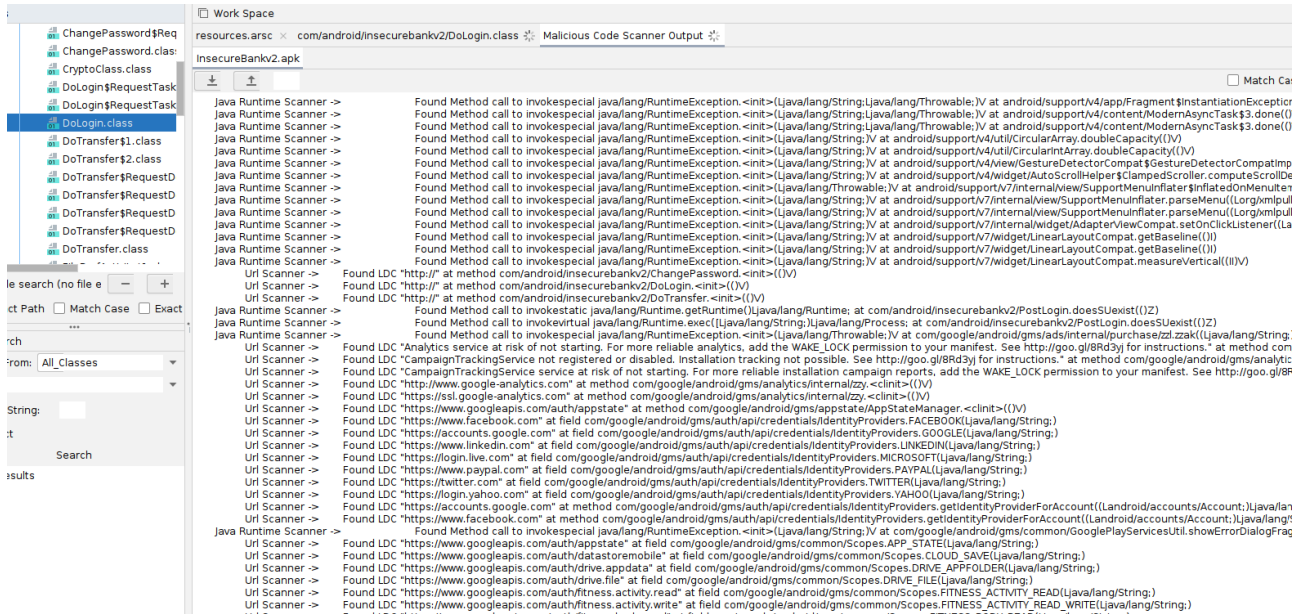
aload 0 // reference to self

ldc Lcom/android/insecurebankv2/FilePrefActivity; (org.objectweb.asm.Type)

invokevirtual android/content/Intent.<init>(Landroid/content/Context;Ljava/l

invokevirtual com/android/insecurebankv2/DoLogin.startActivity(Landroid/cont

Quét các đoạn code có thể là mã độc:

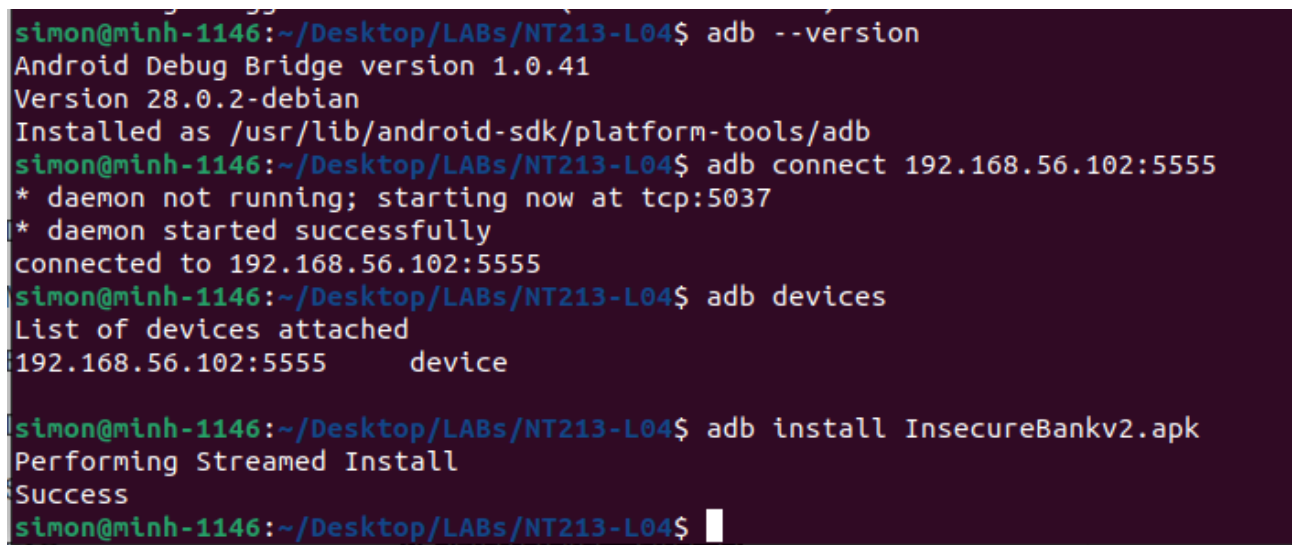


## Phân tích thử file com/android/insecurebankv2/DoLogin\$RequestTask.class

```
public void postData(String var1) throws ClientProtocolException, IOException, JSONException, InvalidKeyException, NoSuchAlgorithmException, NoSuchPaddingException {
    DefaultHttpClient var2 = new DefaultHttpClient();
    HttpPost var4 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/login");
    HttpPost var3 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/devlogin");
    ArrayList var5 = new ArrayList(2);
    var5.add(new BasicNameValuePair("username", this.this$0.username));
    var5.add(new BasicNameValuePair("password", this.this$0.password));
    HttpResponse var6;
    if (this.this$0.username.equals("devadmin")) {
        var3.setEntity(new UrlEncodedFormEntity(var5));
        var6 = var2.execute(var3);
    } else {
        var4.setEntity(new UrlEncodedFormEntity(var5));
        var6 = var2.execute(var4);
    }
}
```

## Yêu cầu 1 Phân tích và chỉ ra điểm bất thường của đoạn code trên?

- Đầu tiên đoạn mã sử dụng HttpPost để post các request đăng nhập. Do không mã hóa đường truyền nên nếu bắt được gói thì thì username và password có thể bị đọc được.
- Và nếu nhập username là devadmin thì có thể login thẳng mà không cần tới password.



**Yêu cầu 2** Chỉ ra rằng dữ liệu lưu trữ có an toàn hay không?

cd data/data/com.android.insecurebankv2/databases

```
simon@minh-1146:~/Desktop/LABs/NT213-L04$ adb shell
genymotion:/ # cd data/data/com.android.insecurebankv2/databases
genymotion:/data/data/com.android.insecurebankv2/databases # sqlite3 mydb
SQLite version 3.18.2 2017-07-21 07:56:09
Enter ".help" for usage hints.
sqlite> .tables
android_metadata  names
sqlite> select * from names
...> ;
sqlite> select * from names;
sqlite> select * from android_metadata;
en_US
sqlite>
```

Không tìm thấy dữ liệu trong database dù đã chạy và kết nối

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:62:e5:65 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.111.128/24 brd 192.168.111.255 scope global dynamic noprefixrou
te ens33
        valid_lft 1055sec preferred_lft 1055sec
        inet6 fe80::6945:c195:e2cf:10b6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP gr
oup default
    link/ether 02:42:a6:78:4b:89 brd ff:ff:ff:ff:ff:ff
7: veth1b82daa@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue mas
ter docker0 state UP group default
    link/ether aa:38:42:5e:a3:a0 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::a838:42ff:fe5e:a3a0/64 scope link
        valid_lft forever preferred_lft forever
simon@minh-1146:~/Desktop/LABs/NT213-L04/AndroLabServer$ python3 app.py
The server is hosted on port: 8888
```

FilePref

Server IP:

Server Port:

Submit



**Yêu cầu 3** Kiểm tra xem thông tin nhạy cảm có lưu lại trên thiết bị hay không? Một số từ khoá: deviceId, userId, imei, deviceSerialNumber, devicePrint, phone, XDSN, mdn, IMSI, uuid...

Không tìm thấy thông tin

```
genymotion:/ # cd /data/data/com.android.insecurebankv2
grep -r "user" $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r "user" $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r "user" $(find)
rep -r "deviceId" $(find)
rep -r "deviceId" $(find)
rep -r "user" $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r "user" $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r "user" $(find)
rep -r "uuid" $(find)
rep -r "deviceSerialNumber" $(find)
1|genymotion:/data/data/com.android.insecurebankv2 #
```

**Yêu cầu 4** Theo bạn thư mục sao lưu chứa thông tin nào cần mã hoá, chỉ ra.

Với quá trình và kết quả thu thập của đề bài, thông tin cần mã hóa là tên của các bảng trong database, tên của các biến quan trọng để tránh dễ bị truy vết

**Yêu cầu 5** Viết chương trình giải mã đoạn dữ liệu mã hoá (python3 chẳng hạn...)

Theo yêu cầu bài thì có key và cipher  
Viết chương trình decrypt:

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
import base64

# Example encrypted data (Base64 encoded)
encrypted_data = "v/sJphdCo2ckDmLWSUwIw==&#10"
key = b'This is the super secret key 123'
iv = b'\x00'*16

# Decode the encrypted data
encrypted_data = base64.b64decode(encrypted_data)

# Create AES cipher
cipher = AES.new(key, AES.MODE_CBC, iv)

# Decrypt and unpad the data
decrypted_data = unpad(cipher.decrypt(encrypted_data), AES.block_size)

print("Decrypted data:", decrypted_data.decode('utf-8'))
```

```
simon@minh-1146: ~/Desktop/LABs/NT213-L04
simon@minh-1146:~/Desktop/LABs/NT213-L04$ python3 decrypt.p
Decrypted data: Jack@123$
simon@minh-1146:~/Desktop/LABs/NT213-L04$
```

### 2. Dịch ngược (Reverse Engineering)

**Yêu cầu 6** Sinh viên điều chỉnh mã nguồn ứng dụng sao cho luôn hiển thị trạng thái “Rooted Device!!” với bất kỳ trạng thái nào của thiết bị.

Sử dụng apktool để dịch ngược apk

```
simon@minh-1146:~/Desktop/LABs/NT213-L04$ /usr/local/bin/apktool d InsecureBankv2.apk
I: Using Apktool 2.9.0 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: /home/simon/.local/share/apktool/framework/1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Truy cập vào InsecureBankv2/smali/com/android/insecurebankv2/ PostLogin.smali để sửa đổi tập tin. Thay đổi để luôn luôn hiện ra “Rooted Device!!”

```
45     move v0, v1
46
47     .line 88
48     .local v0, "isrooted":Z
49     :goto_0
50     if-ne v0, v1, :cond_2
51
52     .line 90
53     iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
54
55     const-string v2, "Rooted Device!!"
56
57     invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
58
59     .line 96
60     :goto_1
61     return-void
62
63     .line 87
64     .end local v0      # "isrooted":Z
65     :cond_1
66     const/4 v0, 0x0
67
68     goto :goto_0
69
70     .line 94
71     .restart local v0      # "isrooted":Z
72     :cond_2
73     iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
74
75     const-string v2, "Device not Rooted!!"
76
77     invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
78
79     goto :goto_1
80 .end method
81
82 .method protected viewStatment()V
83     .locals 3
```

```

    .line 88
    .local v0, "isrooted":Z
    :goto_0
    if-ne v0, v1, :cond_2

    .line 90
   iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;-->root_status:Landroid/widget/TextView;

    const-string v2, "Rooted Device!!"

    invoke-virtual {v1, v2}, Landroid/widget/TextView;-->setText(Ljava/lang/CharSequence;)V

    .line 96
    :goto_1
    return-void

    .line 87
    .end local v0    # "isrooted":Z
    :cond_1
    const/4 v0, 0x0

    goto :goto_0

    .line 94
    .restart local v0    # "isrooted":Z
    :cond_2
    iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;-->root_status:Landroid/widget/TextView;

    const-string v2, "Device Rooted!!"

    invoke-virtual {v1, v2}, Landroid/widget/TextView;-->setText(Ljava/lang/CharSequence;)V

    goto :goto_1
end method

method protected viewStatment()V
    .locals 3

```

### Đóng gói lại file apk

```

simon@minh-1146:~/Desktop/LABs/NT213-L04$ /usr/local/bin/apktool b InsecureBankv
2 -o InsecureBankv3.apk
I: Using Apktool 2.9.0
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building resources...

```

Android yêu cầu các tập tin APK đều phải được ký bằng một chứng chỉ trước khi được phép cài đặt trên thiết bị. Sau khi chỉnh sửa, tập tin APK sẽ không còn toàn vẹn như ban đầu nên cần phải được ký lại. - Vì vậy ta cần tạo key và ký

```

simon@minh-1146:~/Desktop/LABs/NT213-L04$ keytool -genkeypair -v -keystore /home/simon/Desktop/LABs/NT213
-L04/key.keystore -alias InsecureBankv3 -keyalg RSA -keysize 2048 -validity 1000
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: minh vo
What is the name of your organizational unit?
[Unknown]: uit
What is the name of your organization?
[Unknown]: uit
What is the name of your City or Locality?
[Unknown]: hcm
What is the name of your State or Province?
[Unknown]: hcm
What is the two-letter country code for this unit?
[Unknown]: vn
Is CN=minh vo, OU=uit, O=uit, L=hcm, ST=hcm, C=vn correct?
[no]: yes

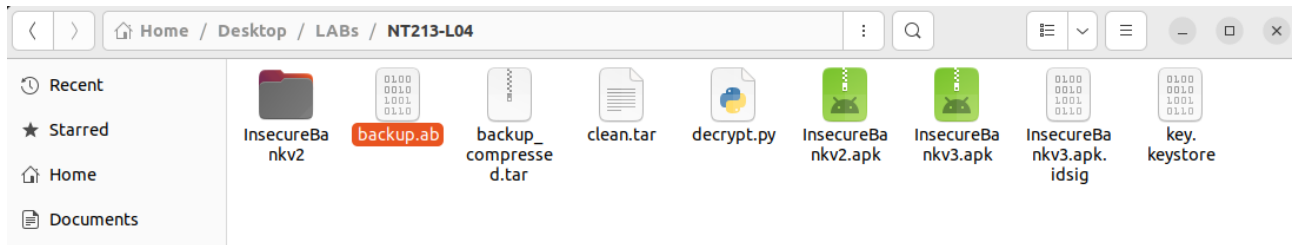
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 1,000 da
ys
for: CN=minh vo, OU=uit, O=uit, L=hcm, ST=hcm, C=vn
[Storing /home/simon/Desktop/LABs/NT213-L04/key.keystore]

```

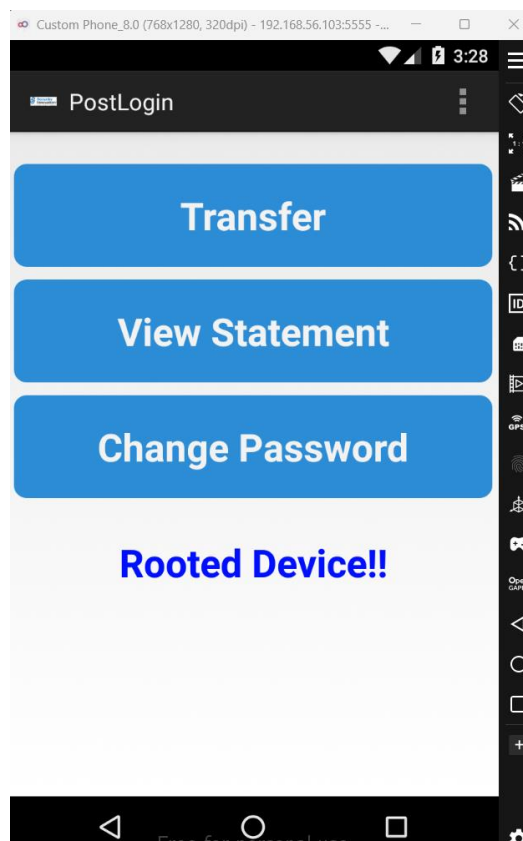


```
simon@minh-1146:~/Desktop/LABs/NT213-L04$ apksigner sign --ks key.keystore InsecureBankv3.apk
Keystore password for signer #1:
```

Đã có một file apk mới

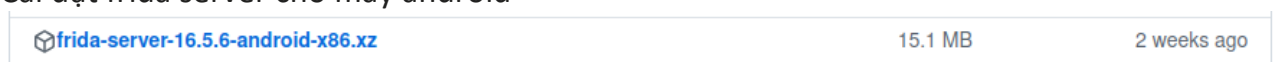


Cài đặt thử, thành công



### 3. Hooking với Frida

Cài đặt frida server cho máy android



```
simon@minh-1146:~/Downloads$ adb push /home/simon/Downloads/frida-server-16.5.6-android-x86.xz /data/local/tmp/frida-server-16.5.6-android-x86.xz
/home/simon/Downloads/frida-server-16.5.6-android-x86.xz 20.8 MB/s (15822100 bytes in 0.726s)
simon@minh-1146:~/Downloads$
```

### Đã kết nối thành công

```
Successfully built frida-tools
Installing collected packages: websockets, frida-tools
Successfully installed frida-tools-13.6.0 websockets-13.1
simon@minh-1146:~/Desktop/LABs/NT213-L04$ frida-ps -U
PID Name
----
2296 Files
1910 Gallery
2824 InsecureBankv2
878 Settings
1602 Superuser
247 adbd
507 android.hardware.camera.provider@2.4-service
508 android.hardware.configstore@1.0-service
simon@minh-1146:~/Desktop/LABs/NT213-L04$ adb shell
genymotion:/ # cd /data/local/tmp/
genymotion:/data/local/tmp # chmod +x frida-server
chmod: frida-server: No such file or directory
genymotion:/data/local/tmp # ls
frida-server-16.5.6-android-x86.xz
genymotion:/data/local/tmp # chmod +x frida-server-16.5.6-android-x86.xz
genymotion:/data/local/tmp # unxz frida-server-16.5.6-android-x86.xz
genymotion:/data/local/tmp # ls
frida-server-16.5.6-android-x86
genymotion:/data/local/tmp # ./frida-server-16.5.6-android-x86
```

### Yêu cầu 7 Hoàn thiện đoạn code trên và demo.

```
1 import frida
2 import time
3
4 device = frida.get_usb_device()
5 pid = device.spawn("com.android.insecurebankv2")
6 device.resume(pid)
7
8 time.sleep(1) # sleep 1 to avoid crash (sometime)
9
10 session=device.attach(pid)
11
12 hook_script="""
13 Java.perform
14 (
15     function()
16     {
17         console.log("Inside the hook_script");
18         classPostLogin = Java.use('com.android.insecurebankv2.PostLogin');
19         classPostLogin.doesSuperuserApkExist.implementation = function()
20         {
21             return true;
22         };
23     }
24 );|
25 """
26
27 script=session.create_script(hook_script)
28 script.load()
29
30 input('...?') # prevent terminate
```

Ở đây ta sẽ ghi đè method `doesSuperuserApkExist()` bằng cách sử dụng `implementation`.

Thực thi code.

```
simon@minh-1146:~/Desktop/LABs/NT213-L04$ python3 hook1.py
Inside the hook_script
...?
38 script.load()
```

---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
  - Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
  - Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).
- Ví dụ: [NT101.K11.ANTT]-Exe01\_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](https://courses.uit.edu.vn).

### Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trể, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**