ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Дисциплина:

«Обеспечение информационной безопасности мобильных устройств»

ОТЧЕТ ПО ЛАБАРАТОРНОЙ РАБОТЕ №2

«Создание приложения и поиск URL, конечных точек и секретов в APK-файлах»

Выполнил:

Гаврилова В. В., студент группы N33471

(подпись)

Проверил:

Федоров Иван Романович

24.02.2022

(отметка о выполнении)

(подпись)

Санкт-Петербург

2022г.

Содержание

1. Цель работы

Ознакомиться с функционалом Android Studio, научиться получать apk файлы, научиться декомпилировать полученный файл с помощью утилиты APKTool, а также ознакомиться с возможностями утилиты APKLeaks.

2. Основная часть

2.1 Описание выбранных средств реализации и обоснования выбора

Для реализации первой части работы был выбран язык программирования Java и Android Studio. Ссылка на туториал по созданию приложения на данном языке программирования была указана в рекомендуемых материалам к лабораторной работе.

Для реализации части 2 была выбрана утилита APKTool (условие лабораторной работы).

Для реализации части 3 была выбрана утилита APKLeaks (условие лабораторной работы).

2.2 Создание проекта и APK файла в Android Studio

Исходный код доступен по ссылке https://github.com/cyberknopa/IS-for-mobile-2022/tree/main/Lab_1

Код файла AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest
xmlns:android="http://schemas.android.com/apk/res/android"
    package="codepath.demos.helloworlddemo"
    android:versionCode="1"
    android:versionName="1.0" >

    <application
        android:allowBackup="true"
        android:icon="@drawable/cat"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity

android:name="codepath.demos.helloworlddemo.N33471_Gavrilova"
            android:label="Student name" >
            <intent-filter>
```

```
                    <action  android:name="android.intent.action.MAIN"
/>

                    <category
android:name="android.intent.category.LAUNCHER" />
                </intent-filter>
            </activity>
        </application>

    </manifest>
```

Код файла N33471_Gavrilova.java

```
    package codepath.demos.helloworlddemo;

    import android.os.Bundle;
    import android.app.Activity;

    public class N33471_Gavrilova extends Activity {

        @Override
        protected void onCreate(Bundle savedInstanceState) {
            super.onCreate(savedInstanceState);
            setContentView(R.layout.gavrilova);
        }

    }
```

Код файла strings.xml

```
    <?xml version="1.0" encoding="utf-8"?>
    <resources>

        <string name="app_name">Gavrilova</string>
        <string name="hello_world">Veronica</string>
        <string name="menu_settings">Settings</string>

    </resources>
```

Код файла gavrilova.xml

```
<RelativeLayout
xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    tools:context=".N33471_Gavrilova" >

    <TextView
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:layout_centerHorizontal="true"
        android:layout_centerVertical="true"
        android:text="N33471 Gavrilova Veronica"
        android:textSize="25sp" />

</RelativeLayout>
```

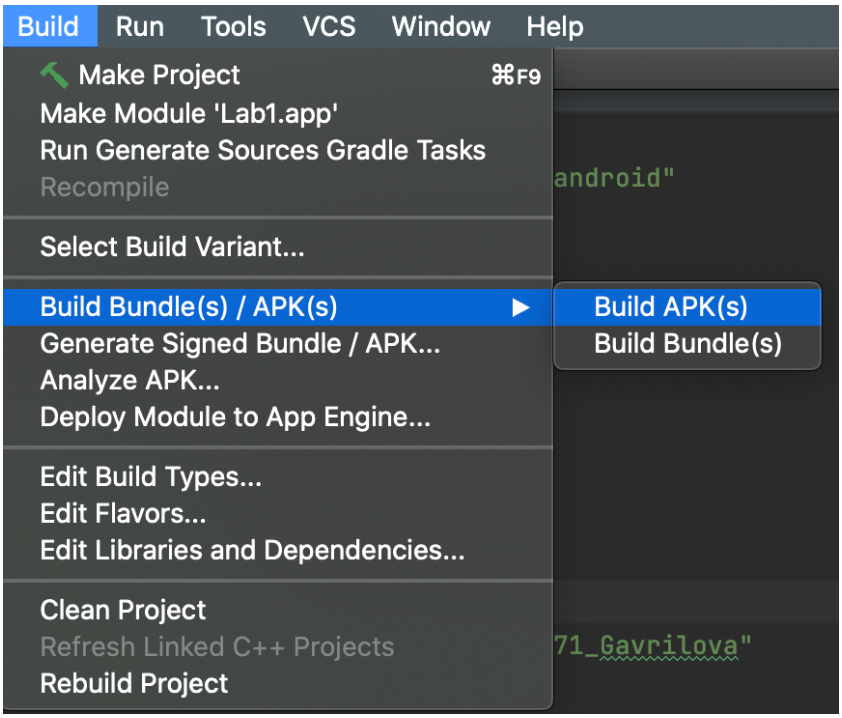

Рисунок 1 – Билд APK файла в Android Studio

Рисунок 2 – Эмулятор

2.3 Декомпиляция APK файла с помощью APKTool

Ссылка на декомпилированный файл https://github.com/cyberknopa/IS-for-mobile-2022/tree/main/Lab1_Decompile

```
MBP-Veronika:Things veronikagavrilova$ apktool d lab.apk
I: Using Apktool 2.6.0 on lab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/veronikagavrilova/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Рисунок 3 – Работа утилиты

```yaml
!!brut.androlib.meta.MetaInfo
apkFileName: lab.apk
compressionType: false
doNotCompress:
- resources.arsc
- png
isFrameworkApk: false
packageInfo:
  forcedPackageId: '127'
  renameManifestPackage: null
sdkInfo:
  minSdkVersion: '21'
  targetSdkVersion: '30'
sharedLibrary: false
sparseResources: false
unknownFiles: {}
usesFramework:
  ids:
  - 1
  tag: null
version: 2.6.0
versionInfo:
  versionCode: '1'
  versionName: '1.0'
```

Рисунок 4 – Файл apktool.yml

2.4 Сканирование APK файла с помощью APKLeaks

Для первого сканирования был выбран APK файл из первой части лабораторной работы.

```
root@kali:~# apkleaks -f '/root/Downloads/lab.apk'
                                                  _
    ___  ____  _  __ _                 _ _ _____
   / _ \ |  _ \| |/ /| |    ___  __ _ | | |  ___|
  / /_\ \| |_) | ' / | |   / _ \/ _` | | | |___
 /  ___  \  __/| . \ | |__|  __/ (_| | |  <\___ \
/_/   \_\_|   |_|\_\|____/\___|\__,_|_|_|\_\___/
 v2.6.1
 --
 Scanning APK file for URIs, endpoints & secrets
 (c) 2020-2021, dwisiswant0

Can't find jadx binary.
Do you want to download jadx? (Y/n) Y

** Downloading jadx...

** Decompiling APK...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
INFO  - loading ...
INFO  - processing ...
INFO  - done

** Scanning against 'codepath.demos.helloworlddemo'

[JSON_Web_Token]
- androidGradlePluginVersion=4.2.2

[LinkFinder]
- http://schemas.android.com/apk/res/android

** Results saved into '/tmp/apkleaks-vn2k9c08.txt'.
```

Рисунок 5 – Работа утилиты

К сожалению, удалось получить только версию сборки и один URL адрес.

[JSON_Web_Token]

- androidGradlePluginVersion=4.2.2

[LinkFinder]

- http://schemas.android.com/apk/res/android

Поэтому для второго сканирования был выбран APK файл Temple-Run-Oz-v1-6-21 rulsmart.com.apk.

Рисунок 6 – Результат работы утилиты

Как можно увидеть, мы получили Artifactory Password, Facebook Secret Key, IP Address и больше количество URL ссылок.

Ссылка на полный отчет https://github.com/cyberknopa/IS-for-mobile-2022/blob/main/Lab1_3/apkleaks-bnhrmid5.txt

[Artifactory_Password]

- AP2tMkmTC0clySJvgUxUmczyyQU

[Facebook_Secret_Key]

- FB_APP_SIGNATURE = "30820268308201d102044a9c4610300d

[IP_Address]

- 1.25.0.3

- 10.0.1.7
- 10.0.2.2
- 192.168.1.1
- 192.168.1.8
- 192.168.2.1

[LinkFinder]
- /1.1/statuses/update_with_media.json
- /Android/data/
- /analytics
- /analytics/
- /android_v2/handle_app_loads
…

3. Вывод

В результате выполнения работы мной были изучены утилиты APKTool и APKLeaks. Так же я научилась создавать простейшее приложение на языке Java и эмулировать его в Android Studio.

4. Источники

[1] https://itsecforu.ru/2021/12/24/🌐-обзор-проверенных-способов-поиска/