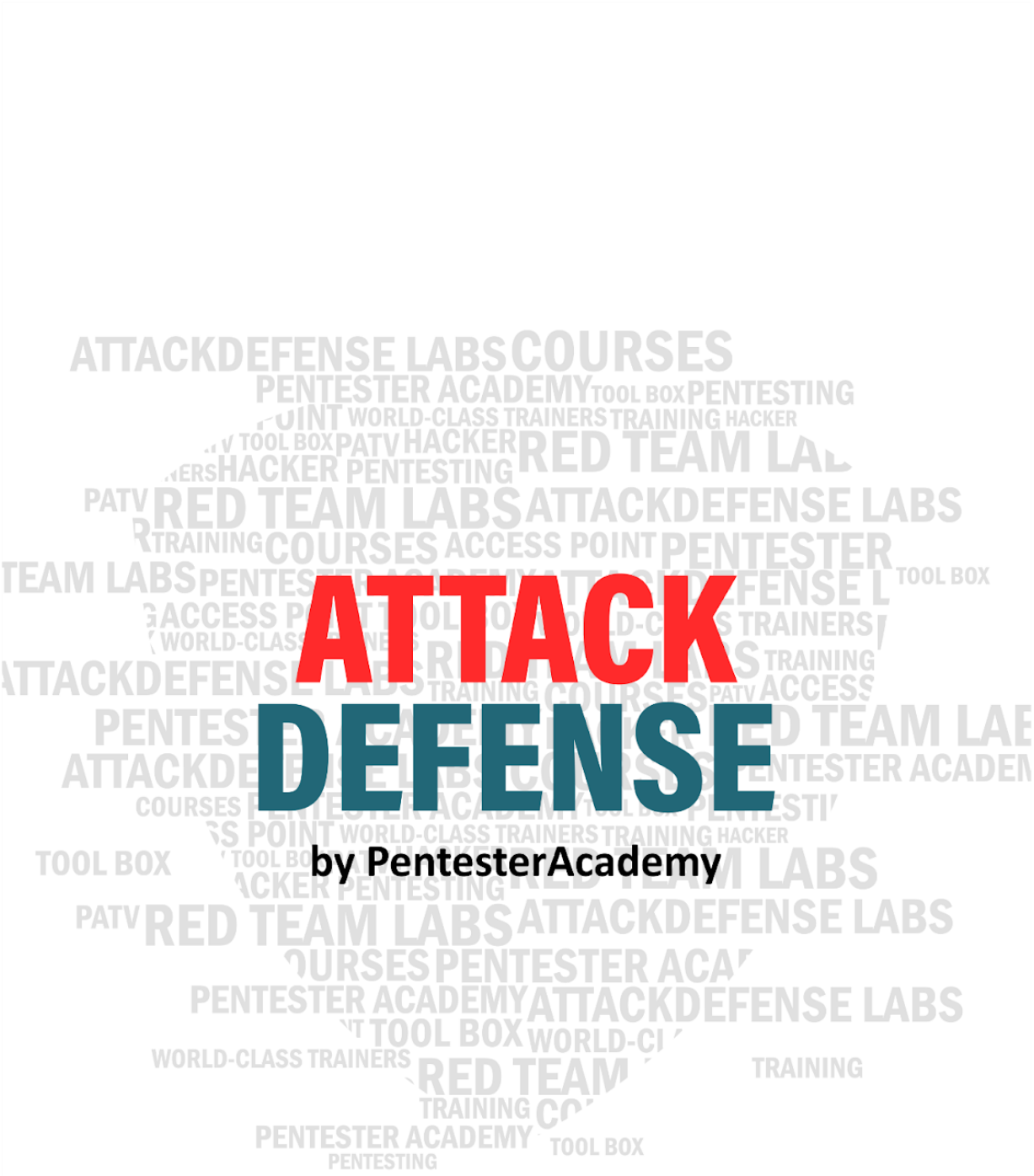
ATTACK
DEFENSE
by PentesterAcademy

Name	Understanding AndroidManifest.xml
URL	https://attackdefense.com/challengedetails?cid=1622
Type	Android Pentesting : Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: AndroidManifest.xml of an android application is provided in the lab. Analyze the file and answer the following questions regarding :

Solution:

Start the lab and check the contents of the home directory.

Command: ls -l

```
root@attackdefense:~# ls -l
total 60
-rw-r--r-- 1 root root 60404 Jan 23 07:03 sample-app.apk
root@attackdefense:~#
```

Open the APK using apktool

Command: apktool d sample-app.apk

```
root@attackdefense:~# apktool d sample-app.apk
I: Using Apktool 2.4.1 on sample-app.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
root@attackdefense:~#
```

Apktool will extract all files in a new directory. Open the AndroidManifest.xml file

Command: vim sample-app/AndroidManifest.xml

```
root@attackdefense:~# ls -l
total 64
drwxr-xr-x 5 root root  4096 Jan 23 07:53 sample-app
-rw-r--r-- 1 root root 60404 Jan 23 07:03 sample-app.apk
root@attackdefense:~#
root@attackdefense:~# vim sample-app/AndroidManifest.xml
```

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="23" android:compileSdkVersionCodename="6.0-2438415" package="com.example.sampleapp" platformBuildVersionCode="23" platformBuildVersionName="6.0-2438415">
    <uses-feature android:name="android.hardware.sensor.compass" android:required="true"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@style/AppTheme">
        <activity android:label="@string/app_name" android:name="com.example.sampleapp.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <service android:enabled="true" android:exported="true" android:name=".ReService"/>
    </application>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
</manifest>
```

Q.1: What is the name of the application?

Answer: sampleapp

Solution:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
rsion="23" android:compileSdkVersionCodename="6.0-2438415" package="com.example.sampleapp" platformBuildVersionCode="23" pl
me="6.0-2438415">
```

Q.2: What is the version of the SDK on which this app was compiled?

Answer: 23

Solution:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVe
rsion="23" android:compileSdkVersionCodename="6.0-2438415" package="com.example.sampleapp" platformBuildVersionCode="23" platformBuildVersionNa
me="6.0-2438415">
```

Q.3: How many permission elements are present in the file?

Answer: 4

Solution:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVe
rsion="23" android:compileSdkVersionCodename="6.0-2438415" package="com.example.sampleapp" platformBuildVersionCode="23" platformBuildVersionNa
me="6.0-2438415">
    <uses-feature android:name="android.hardware.sensor.compass" android:required="true"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@style/AppTheme"
>
        <activity android:label="@string/app_name" android:name="com.example.sampleapp.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <service android:enabled="true" android:exported="true" android:name=".ReService"/>
    </application>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
</manifest>
```

Q.4: Is it possible to take a backup of this application via ADB?

Answer: Yes

Solution:

android:allowBackup=”true” allows a user to take backup of this application using ADB.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVe
rsion="23" android:compileSdkVersionCodename="6.0-2438415" package="com.example.sampleapp" platformBuildVersionCode="23" platformBuildVersionNa
me="6.0-2438415">
    <uses-feature android:name="android.hardware.sensor.compass" android:required="true"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@style/AppTheme"
>
        <activity android:label="@string/app_name" android:name="com.example.sampleapp.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <service android:enabled="true" android:exported="true" android:name=".ReService"/>
    </application>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
</manifest>
```

Q.5: The application has a service. Can this service be invoked by the components of other applications?

Answer: Yes

Solution:

android.exported=[“true”] allows this service to be invoked by external components.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVe
rsion="23" android:compileSdkVersionCodename="6.0-2438415" package="com.example.sampleapp" platformBuildVersionCode="23" platformBuildVersionNa
me="6.0-2438415">
    <uses-feature android:name="android.hardware.sensor.compass" android:required="true"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@style/AppTheme"
>
        <activity android:label="@string/app_name" android:name="com.example.sampleapp.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <service android:enabled="true" android:exported="true" android:name=".ReService"/>
    </application>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
</manifest>
```

References:

1. AndroidManifest.xml (https://developer.android.com/guide/topics/manifest/manifest-intro)