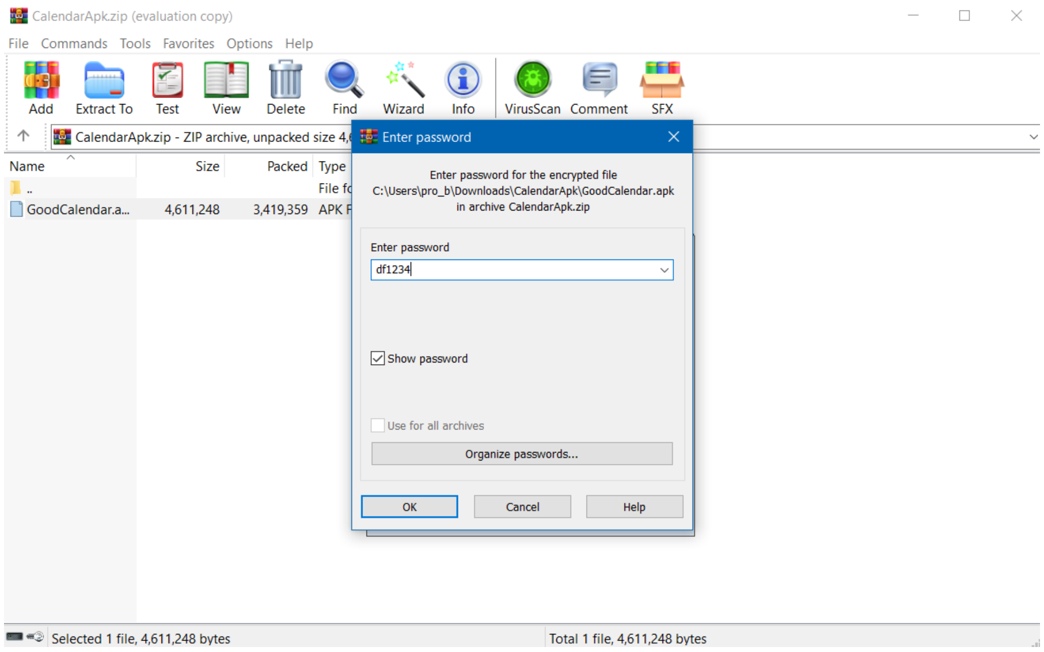
Malicious APK File Analysis

No. 10

Step 1) downloaded the file



CalendarApk.zip (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

CalendarApk.zip - ZIP archive, unpacked size 4,

Name	Size	Packed	Type
..			File fo
GoodCalendar.a...	4,611,248	3,419,359	APK F

Enter password

Enter password for the encrypted file
C:\Users\pro_b\Downloads\CalendarApk\GoodCalendar.apk
in archive CalendarApk.zip

Enter password
df1234

[✓] Show password

[ ] Use for all archives

Organize passwords...

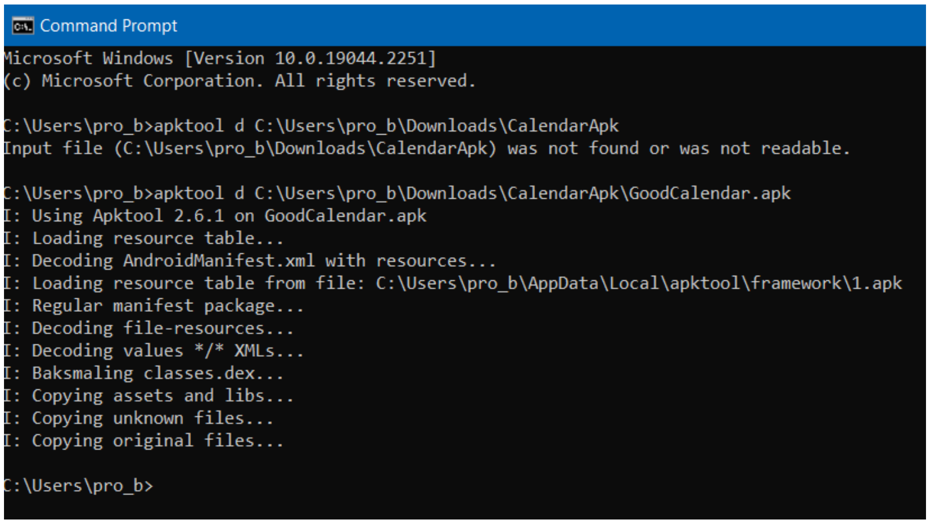
OK Cancel Help

Selected 1 file, 4,611,248 bytes   Total 1 file, 4,611,248 bytes

Step 2) Next, I used APKTool in the Command Prompt to unpack the .apk file into subfolders (original, res, smali, etc) which I could then look through and analyze. The command I used is:

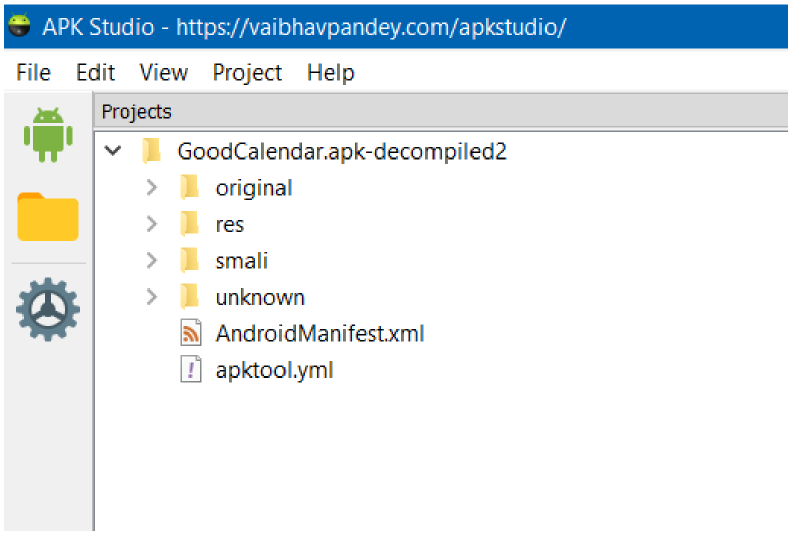
apktook d "path to .apk file"

The unpacked folder will then appear in the same folder that the original .apk file was located in.



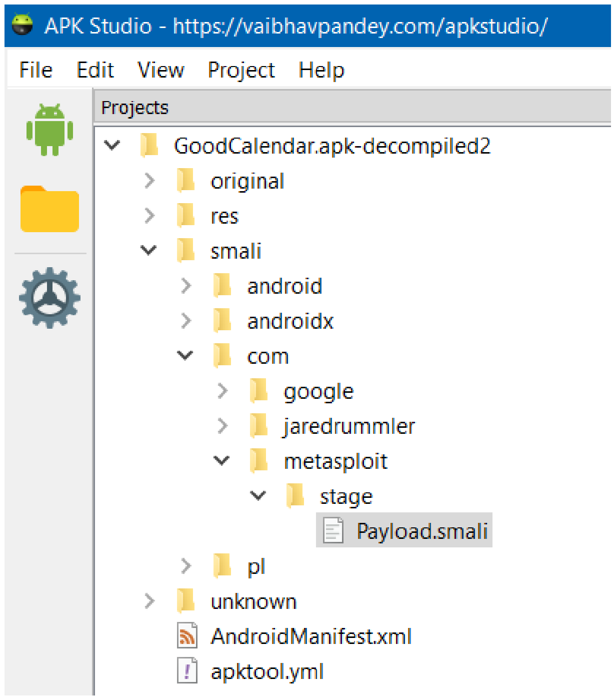
```
Command Prompt
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pro_b>apktool d C:\Users\pro_b\Downloads\CalendarApk
Input file (C:\Users\pro_b\Downloads\CalendarApk) was not found or was not readable.

C:\Users\pro_b>apktool d C:\Users\pro_b\Downloads\CalendarApk\GoodCalendar.apk
I: Using Apktool 2.6.1 on GoodCalendar.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\pro_b\AppData\Local\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...

C:\Users\pro_b>
```

Step 3) Then, I opened up the unpacked .apk file in APK Studio, which allows me to decompile the resource, smali, and java files in order to make them readable and analyzable. APK Studio allows for easy reading and editing of the decompiled files contained in the apk.



```
GoodCalendar.apk-decompiled2
    original
    res
    smali
    unknown
    AndroidManifest.xml
    apktool.yml
```

Step 4) I first looked through the smali folder. I figured that most malicious files should be stored in here, as that was the folder that I put my malicious code into for my own malicious .apk file. In the smali folder, I was able to find a metasploit folder with a Payload file contained in it. It is highly likely that this is the injected malicious code.

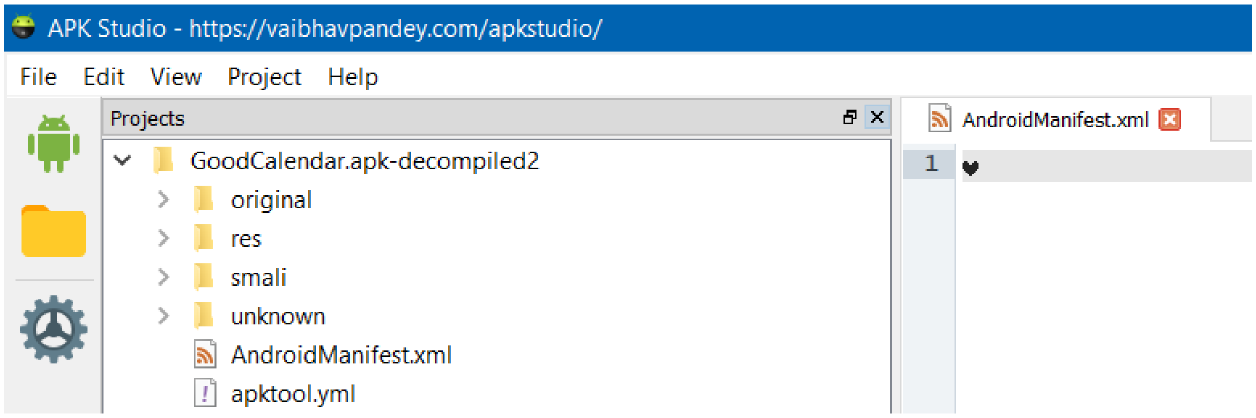


```
GoodCalendar.apk-decompiled2
    original
    res
    smali
        android
        androidx
        com
            google
            jaredrummler
            metasploit
                stage
                    Payload.smali
        pl
    unknown
    AndroidManifest.xml
    apktool.yml
```

Step 5) Upon looking through the payload.smali file and analyzing the code, I was able to tell that this payload file probably creates a simple buffer overload, similar to the payload we created in the malicious .pdf assignment. Buffer overloads occur when the volume of data exceeds the memory capacity of the buffer, which can cause the program to crash or execute other code included in the files.

```
# direct methods
.method static constructor <clinit>()V
    .locals 1

    const/16 v0, 0x2004

    new-array v0, v0, [B

    fill-array-data v0, :array_0

    sput-object v0, Lcom/metasploit/stage/Payload;->a:[B

    return-void

    :array_0
    .array-data 1
        0x4t
        0x0t
        0x0t
        0x0t
        0x0t
        0x0t
        0x0t
        0x0t
        0x0t
        0x0t
```

Step 6) Finally, for the secret code, I was able to find this heart symbol in the AndroidManifest.xml file in the “original” folder. This AndroidManifest is different from the other AndroidManifest file in the decompiled .apk folder. I was not able to find any other secret codes or out of place strings anywhere else in the hundreds of files located within the .apk, so I think that it is safe to assume that this heart symbol is the secret code.



```
GoodCalendar.apk-decompiled2
    original
    res
    smali
    unknown
    AndroidManifest.xml
    apktool.yml
```

```
♥
```