Malicious APK File Analysis
No. 3

Secret Code is **Your Secret is Out**

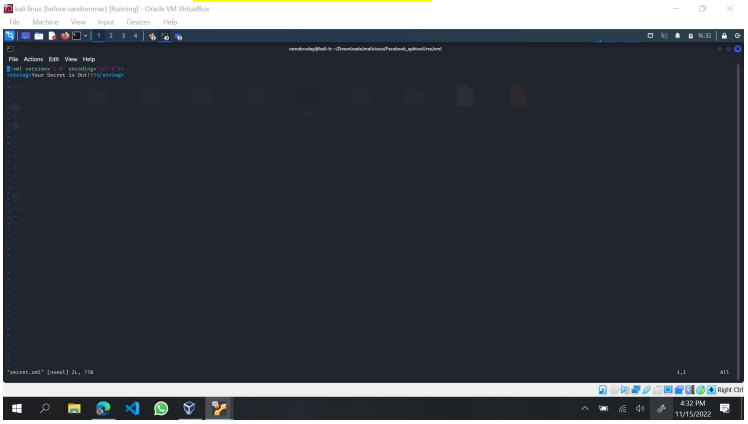

Figure 1 Secret.xml

Analysis Performed

1. Is the sample obfuscated, and if so, which techniques were used to unhide?
   The sample is not obfuscated.
   Using androguard to decrypt android.xml file, below is the screenshot

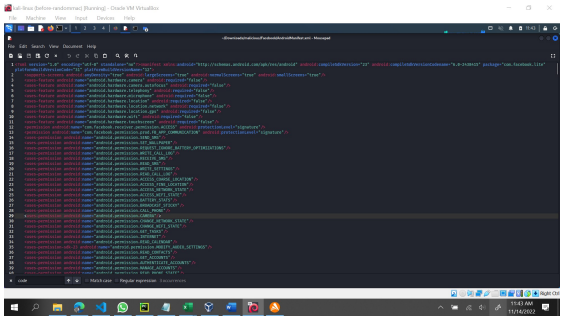

Figure 2 AndroidManifest.xml of the given apk

2. What the normal part of the code does?
   The normal part of the code is Facebook app where we can create Facebook account and access our Facebook account. It's a light version of Facebook app called Facebook lite.

3. What the malicious part of the code does?
   The malicious part of the code opens up the reverse shell connection aka connect-back which requires the attacker to set up a listener first on his box, the target machine acts as a client connecting to that listener, and then finally, the attacker receives the shell.
   We also found IP addresses and tcp connection code which links to **payload/android/meterpreter/reverse_tcp.** Screenshot below.

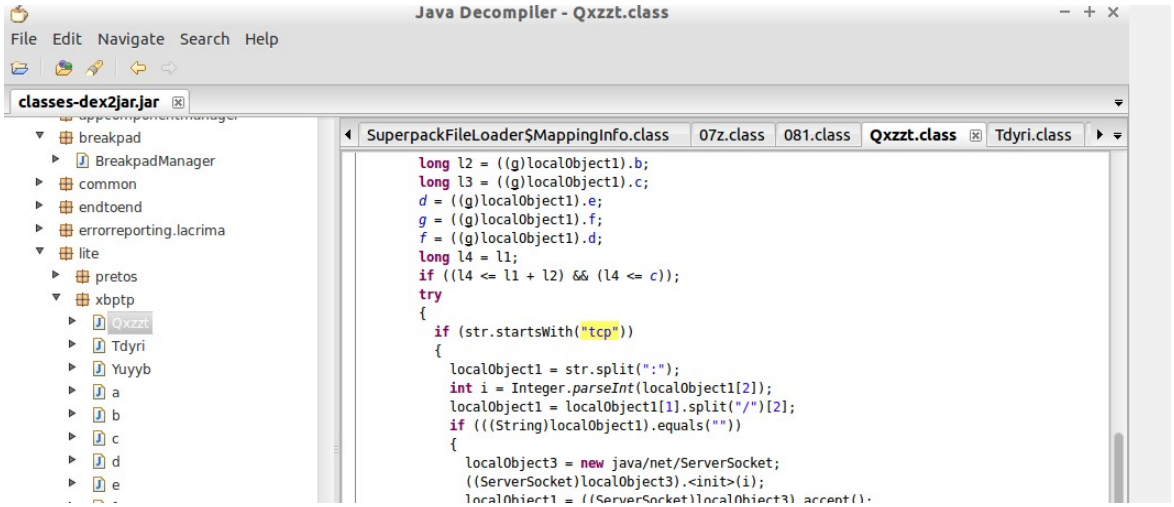

Figure 3 Suspicious TCP connection using server socket

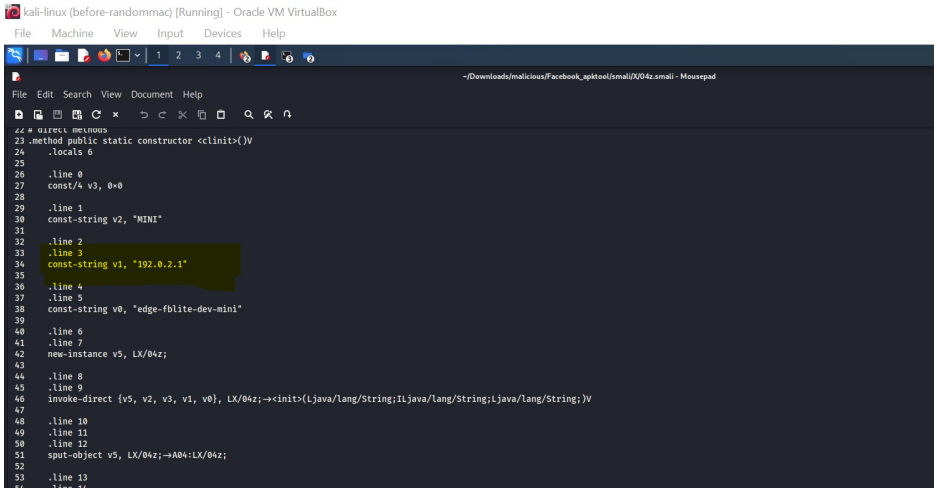

Figure 4 IP address found, linking to reverse_tcp exploit of metasploit

4. Provide some snapshots of your dissected Java code using JD-GUI.

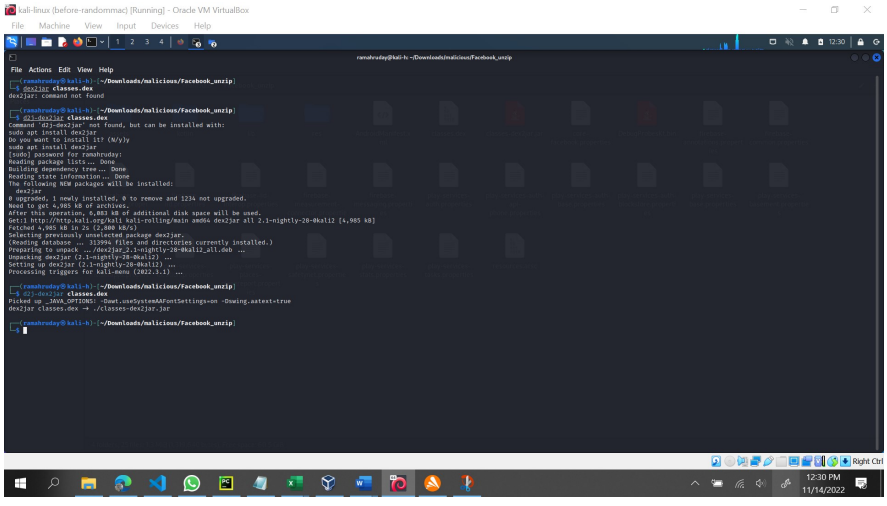

Figure 5 Convert classes.dex to jar

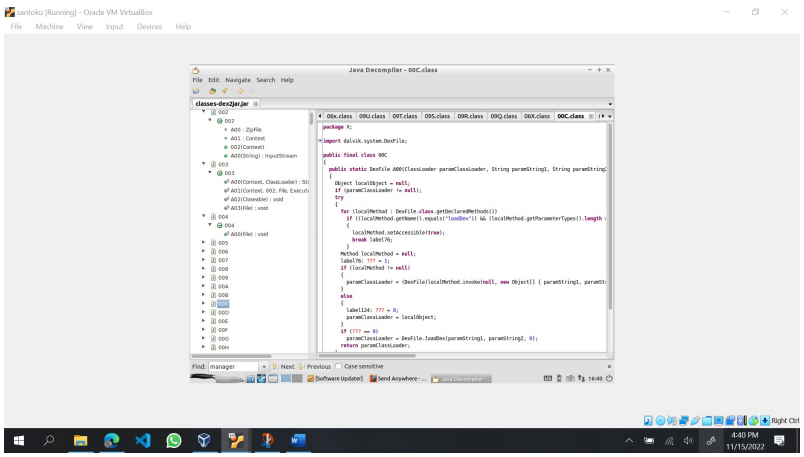

Figure 6 dex2jar visa JD-GUI

5. What kind of permissions this app needs?

['android.permission.CAMERA', 'android.permission.WRITE_CALL_LOG', 'com.facebook.wakizashi.provider.ACCESS', 'android.permission.READ_PHONE_STATE', 'android.permission.RECEIVE_SMS', 'android.permission.ACCESS_COARSE_LOCATION', 'android.permission.READ_CALENDAR', 'android.permission.SYSTEM_ALERT_WINDOW', 'com.sonymobile.home.permission.PROVIDER_INSERT_BADGE', 'android.permission.CALL_PHONE', 'android.permission.FOREGROUND_SERVICE', 'android.permission.READ_PHONE_NUMBERS', 'android.permission.SEND_SMS', 'android.permission.WAKE_LOCK', 'android.permission.RECEIVE_BOOT_COMPLETED', 'com.sonyericsson.home.permission.BROADCAST_BADGE', 'android.permission.BATTERY_STATS', 'android.permission.AUTHENTICATE_ACCOUNTS', 'com.sec.android.provider.badge.permission.WRITE', 'com.facebook.katana.provider.ACCESS', 'android.permission.ACCESS_WIFI_STATE', 'android.permission.READ_PROFILE', 'android.permission.WRITE_CALENDAR','com.sec.android.provider.badge.permission.READ', 'android.permission.GET_ACCOUNTS', 'android.permission.WRITE_CONTACTS', 'android.permission.VIBRATE', 'com.facebook.services.identity.FEO2', 'android.permission.ACCESS_FINE_LOCATION', 'com.facebook.permission.prod.FB_APP_COMMUNICATION', 'android.permission.GET_TASKS', 'android.permission.CHANGE_NETWORK_STATE', 'com.huawei.android.launcher.permission.READ_SETTINGS', 'android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS', 'android.permission.WRITE_SETTINGS','android.permission.READ_SMS', 'android.permission.ACCESS_NETWORK_STATE', 'android.permission.RECORD_AUDIO','com.facebook.orca.provider.ACCESS', 'android.permission.READ_CALL_LOG', 'com.htc.launcher.permission.READ_SETTINGS','com.htc.launcher.permission.UPDATE_SHORTCUT', 'com.huawei.android.launcher.permission.CHANGE_BADGE', 'android.permission.WRITE_EXTERNAL_STORAGE', 'android.permission.SET_WALLPAPER', 'android.permission.MANAGE_ACCOUNTS','com.huawei.android.launcher.permission.WRITE_SETTINGS', 'com.android.launcher.permission.UNINSTALL_SHORTCUT','android.permission.USE_FULL_SCREEN_INTENT', 'android.permission.CHANGE_WIFI_STATE','com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE', 'android.permission.BROADCAST_STICKY', 'com.google.android.c2dm.permission.RECEIVE', 'com.android.launcher.permission.INSTALL_SHORTCUT', 'com.facebook.receiver.permission.ACCESS', 'com.oppo.launcher.permission.READ_SETTINGS', 'android.permission.READ_CONTACTS', 'com.oppo.launcher.permission.WRITE_SETTINGS', 'android.permission.REORDER_TASKS', 'com.facebook.mlite.provider.ACCESS', 'android.permission.INTERNET']

6. What activities are listed in this apk file?

'com.facebook.lite.ShortcutLauncherActivity', 'com.facebook.lite.ShortcutActivity', 'com.facebook.lite.rtc.RTCActivity', 'com.facebook.lite.webviewrtc.RTCIncomingCallActivity', 'com.facebook.lite.nativeRtc.NativeRtcCallActivity', 'com.facebook.lite.media.AlbumGalleryActivity', 'com.facebook.lite.photo.PreviewActivity', 'com.facebook.lite.platform.LoginGDPDialogActivityV2', 'com.facebook.lite.storagemanager.ManageStorageActivity', 'com.facebook.lite.bugreporter.screencast.ScreencastActivity', 'com.facebook.lite.inappbrowser.common.BrowserLiteProxyActivity', 'com.facebook.browser.lite.BrowserLiteActivity', 'com.facebook.browser.lite.BrowserLiteInMainProcessActivity', 'com.facebook.lite.deeplinking.UIQRE2EActivity', 'com.facebook.lite.waotp.WAOtpReceiveCodeActivity', 'com.google.android.gms.auth.api.signin.internal.SignInHubActivity']