

Android Security & Exploitation



Aditya Gupta (@adi1391)

Founder, Attify (<http://attify.com>)

adi@attify.com

Certifications : <http://securitytube-training.com>

Pentester Academy : <http://PentesterAcademy.com>

Androguard 101

- Reverse Engineering and Malware Analysis framework
- Open Source
- Really handy for analyzing applications
- <https://github.com/androguard/androguard>

Getting Started

- Load up Androguard - Androlyze
- Get all the activities, permissions and services
- How to find classes and methods?
- What about source code ?

Getting Started

- `androlyze -s`
- `myapp = APK('/absolute/path/of/apk')`
- `myapp.get_activities()`
- `myapp.get_permissions()`

Finding Activities

```
In [4]: sample.get_activities()
Out[4]:
['com.threebanana.notes.Notes',
'com.threebanana.notes.Migrator',
'com.threebanana.notes.PasscodeActivity',
'com.threebanana.notes.NoteList',
'com.threebanana.notes.NoteEditor',
'com.threebanana.notes.BananaSearchLabels',
'com.threebanana.notes.NotePreferences',
'com.threebanana.notes.BananaGallery',
'com.threebanana.notes.ViewImage',
'com.threebanana.notes.MediaMover',
'com.threebanana.notes.ClearNotes',
'com.threebanana.notes.LauncherShortcuts',
'com.threebanana.notes.SetReminder']
```

Finding Services

```
In [19]: sample.get_services()  
Out[19]:  
['com.threebanana.service.ReminderService',  
'com.catchnotes.sync.SyncService',  
'com.threebanana.service.ExportService']
```

Finding permissions

```
In [20]: sample.get_permissions()
Out[20]:
['android.permission.INTERNET',
'android.permission.CAMERA',
'android.permission.VIBRATE',
'android.permission.WRITE_SETTINGS',
'android.permission.WRITE_EXTERNAL_STORAGE',
'android.permission.ACCESS_NETWORK_STATE',
'android.permission.ACCESS_COARSE_LOCATION',
'android.permission.ACCESS_FINE_LOCATION',
'android.permission.RECEIVE_BOOT_COMPLETED',
'com.android.launcher.permission.INSTALL_SHORTCUT',
'com.android.launcher.permission.UNINSTALL_SHORTCUT',
'com.catchnotes.permission.ACTIVITY']
```

Identifying Content Providers

```
In [21]: sample.get_providers()  
Out[21]:  
['com.threebanana.notes.NotePadProvider',  
 'com.threebanana.notes.NotePadPendingProvider']
```


And a lot more

```
In [22]: sample.  
sample.androidversion  
sample.arsc  
sample.axml  
sample.filename  
sample.files  
sample.files_crc32  
sample.format_value  
sample.get_AndroidManifest  
sample.get_activities  
sample.get_android_manifest_axml  
sample.get_android_manifest_xml  
sample.get_android_resources  
sample.get_androidversion_code  
sample.get_androidversion_name  
sample.get_certificate  
sample.get_details_permissions  
sample.get_dex  
sample.get_element  
sample.get_elements  
sample.get_file  
sample.get_filename  
sample.get_files  
sample.get_files_crc32  
sample.get_files_information  
sample.get_files_types  
sample.get_intent_filters  
sample.get_libraries  
sample.get_main_activity  
sample.get_max_sdk_version  
sample.get_min_sdk_version  
sample.get_package  
sample.get_permissions  
sample.get_providers  
sample.get_raw  
sample.get_receivers  
sample.get_services  
sample.get_signature  
sample.get_signature_name  
sample.get_target_sdk_version  
sample.is_valid_APK  
sample.magic_file  
sample.new_zip  
sample.package  
sample.permissions  
sample.show  
sample.valid_apk  
sample.xml  
sample.zip  
sample.zipmodule
```

Getting XML of Manifest

```
In [22]: sample.  
sample.androidversion  
sample.arsc  
sample.axml  
sample.filename  
sample.files  
sample.files_crc32  
sample.format_value  
sample.get_AndroidManifest  
sample.get_activities  
sample.get_android_manifest_axml  
sample.get_android_manifest_xml  
sample.get_android_resources  
sample.get_androidversion_code  
sample.get_androidversion_name  
sample.get_certificate  
sample.get_details_permissions  
sample.get_dex  
sample.get_element  
sample.get_elements  
sample.get_file  
sample.get_filename  
sample.get_files  
sample.get_files_crc32  
sample.get_files_information  
sample.get_files_types  
sample.get_intent_filters  
sample.get_libraries  
sample.get_main_activity  
sample.get_max_sdk_version  
sample.get_min_sdk_version  
sample.get_package  
sample.get_permissions  
sample.get_providers  
sample.get_raw  
sample.get_receivers  
sample.get_services  
sample.get_signature  
sample.get_signature_name  
sample.get_target_sdk_version  
sample.is_valid_APK  
sample.magic_file  
sample.new_zip  
sample.package  
sample.permissions  
sample.show  
sample.valid_apk  
sample.xml  
sample.zip  
sample.zipmodule
```

Gives you Manifest in xml

Application Permission Details

```
In [22]: sample.  
sample.androidversion  
sample.arsc  
sample.axml  
sample.filename  
sample.files  
sample.files_crc32  
sample.format_value  
sample.get_AndroidManifest  
sample.get_activities  
sample.get_android_manifest_axml  
sample.get_android_manifest_xml  
sample.get_android_resources  
sample.get_androidversion_code  
sample.get_androidversion_name  
sample.get_certificate  
sample.get_details_permissions  
sample.get_dex  
sample.get_element  
sample.get_elements  
sample.get_file  
sample.get_filename  
sample.get_files  
sample.get_files_crc32  
sample.get_files_information  
sample.get_files_types  
sample.get_intent_filters  
sample.get_libraries  
sample.get_main_activity  
sample.get_max_sdk_version  
sample.get_min_sdk_version  
sample.get_package  
sample.get_permissions  
sample.get_providers  
sample.get_raw  
sample.get_receivers  
sample.get_services  
sample.get_signature  
sample.get_signature_name  
sample.get_target_sdk_version  
sample.is_valid_APK  
sample.magic_file  
sample.new_zip  
sample.package  
sample.permissions  
sample.show  
sample.valid_apk  
sample.xml  
sample.zip  
sample.zipmodule
```

All the permissions and details

Files

```
In [22]: sample.  
sample.androidversion  
sample.arsc  
sample.axml  
sample.filename  
sample.files  
sample.files_crc32  
sample.format_value  
sample.get_AndroidManifest  
sample.get_activities  
sample.get_android_manifest_axml  
sample.get_android_manifest_xml  
sample.get_android_resources  
sample.get_androidversion_code  
sample.get_androidversion_name  
sample.get_certificate  
sample.get_details_permissions  
sample.get_dex  
sample.get_element  
sample.get_elements  
sample.get_file  
sample.get_filename  
sample.get_files  
sample.get_files_crc32  
sample.get_files_information  
sample.get_files_types  
sample.get_intent_filters  
sample.get_libraries  
sample.get_main_activity  
sample.get_max_sdk_version  
sample.get_min_sdk_version  
sample.get_package  
sample.get_permissions  
sample.get_providers  
sample.get_raw  
sample.get_receivers  
sample.get_services  
sample.get_signature  
sample.get_signature_name  
sample.get_target_sdk_version  
sample.is_valid_APK  
sample.magic_file  
sample.new_zip  
sample.package  
sample.permissions  
sample.show  
sample.valid_apk  
sample.xml  
sample.zip  
sample.zipmodule
```

All the files inside the APK package

Package Name

```
In [22]: sample.  
sample.androidversion  
sample.arsc  
sample.axml  
sample.filename  
sample.files  
sample.files_crc32  
sample.format_value  
sample.get_AndroidManifest  
sample.get_activities  
sample.get_android_manifest_axml  
sample.get_android_manifest_xml  
sample.get_android_resources  
sample.get_androidversion_code  
sample.get_androidversion_name  
sample.get_certificate  
sample.get_details_permissions  
sample.get_dex  
sample.get_element  
sample.get_elements  
sample.get_file  
sample.get_filename  
sample.get_files  
sample.get_files_crc32  
sample.get_files_information  
sample.get_files_types  
sample.get_intent_filters  
sample.get_libraries  
sample.get_main_activity  
sample.get_max_sdk_version  
sample.get_min_sdk_version  
sample.get_package  
sample.get_permissions  
sample.get_providers  
sample.get_raw  
sample.get_receivers  
sample.get_services  
sample.get_signature  
sample.get_signature_name  
sample.get_target_sdk_version  
sample.is_valid_APK  
sample.magic_file  
sample.new_zip  
sample.package  
sample.permissions  
sample.show  
sample.valid_apk  
sample.xml  
sample.zip  
sample.zipmodule
```

Package Name

Whether a valid APK or not

```
In [22]: sample.  
sample.androidversion  
sample.arsc  
sample.axml  
sample.filename  
sample.files  
sample.files_crc32  
sample.format_value  
sample.get_AndroidManifest  
sample.get_activities  
sample.get_android_manifest_axml  
sample.get_android_manifest_xml  
sample.get_android_resources  
sample.get_androidversion_code  
sample.get_androidversion_name  
sample.get_certificate  
sample.get_details_permissions  
sample.get_dex  
sample.get_element  
sample.get_elements  
sample.get_file  
sample.get_filename  
sample.get_files  
sample.get_files_crc32  
sample.get_files_information  
sample.get_files_types  
sample.get_intent_filters  
sample.get_libraries  
sample.get_main_activity  
sample.get_max_sdk_version  
sample.get_min_sdk_version  
sample.get_package  
sample.get_permissions  
sample.get_providers  
sample.get_raw  
sample.get_receivers  
sample.get_services  
sample.get_signature  
sample.get_signature_name  
sample.get_target_sdk_version  
sample.is_valid_APK  
sample.magic_file  
sample.new_zip  
sample.package  
sample.permissions  
sample.show  
sample.valid_apk  
sample.xml  
sample.zip  
sample.zipmodule
```

Whether a valid APK

Retrieving all classes

- `d = dvm.DalvikVMFormat(myapp.get_dex())`

Retrieving all classes

Dalvik Virtual Machine

Getting DEX content

- `d = dvm.DalvikVMFormat(myapp.get_dex())`

App instance we created earlier

Retrieving all classes

Print out all the class names

- `for class in d.get_classes():
 print class.get_name()`

Retrieving all classes

Print out all the method names

- `for method in d.get_methods():`
 `print class.get_name()`

ATTIFY
HANDS-ON LAB

**Print methods corresponding to
each class**