IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

Construyendo un laboratorio de análisis de aplicaciones Android

CENTRO CRIPTOLÓGICO NACIONAL

- María Isabel Rojo
- Software Security Assurance Team - Indra
- mirojo@indra.es

Índice

¿Por qué Android?

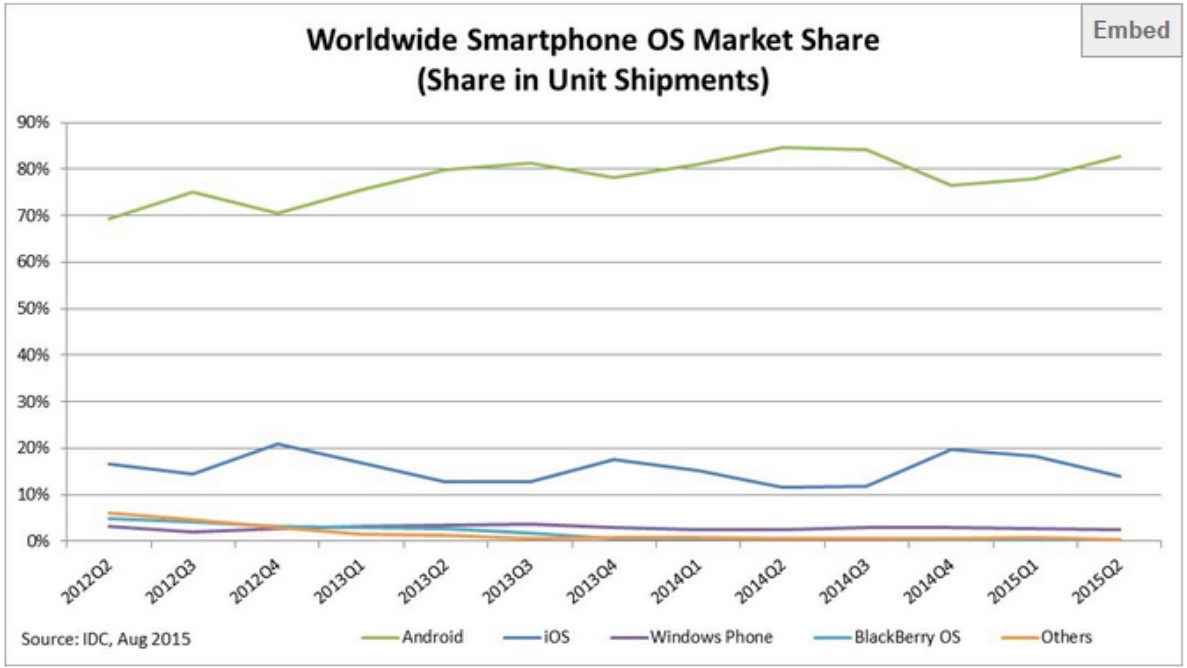
Por qué un laboratorio para Android

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

Source: IDC, Aug 2015

¿Por qué Android?

Por qué un laboratorio para Android



Problemática

Primeros problemas

- Decenas de herramientas
- Desactualizadas / Abandonadas
- Rápida evolución de Android
- Nuevo malware, misma finalidad

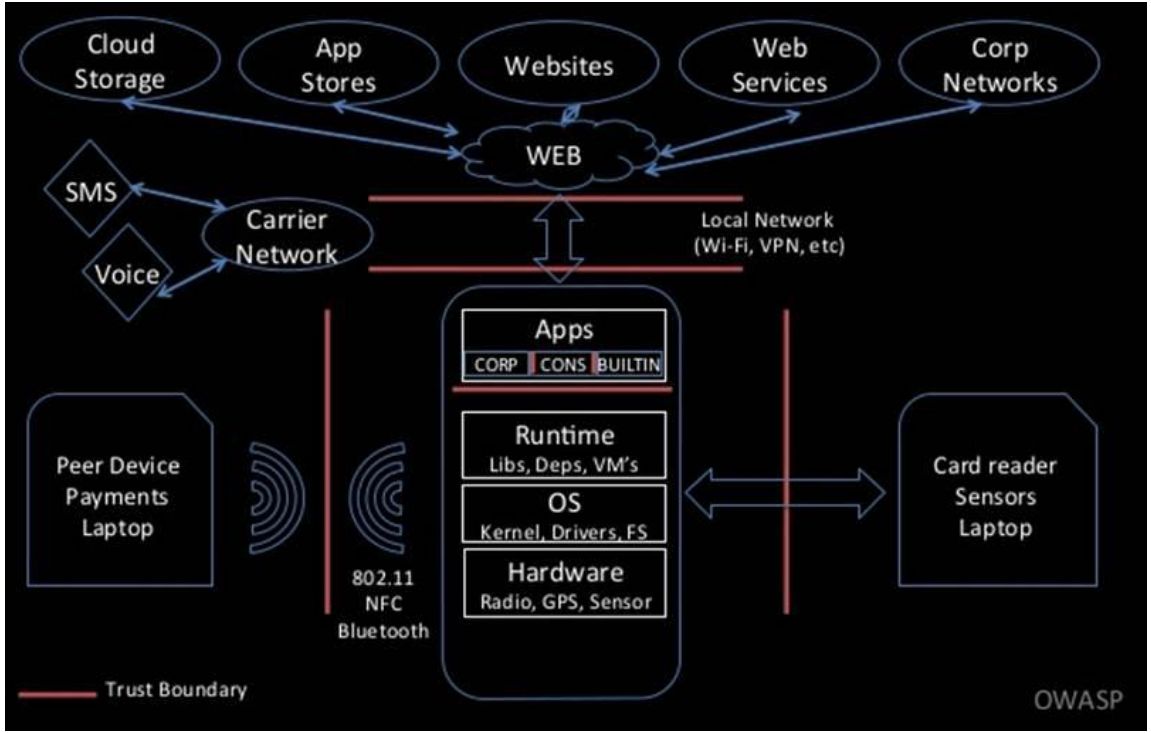
¿Qué?

¿Qué atacar en un pentesting?

- Superficie de ataque o funcionalidad
- Interacción con otros componentes
  - Interacción con los componentes IPC
  - Permisos
  - Funcionalidades expuestas
- Comunicaciones
  - Secure channel
- Datos
- Interacción con el navegador – Get, Post
- Vulnerabilidades
  - Java o vulnerabilidades del lenguaje
  - Dependencias externas vulnerables/desactualizadas

¿Qué?

¿Qué atacar en un pentesting?



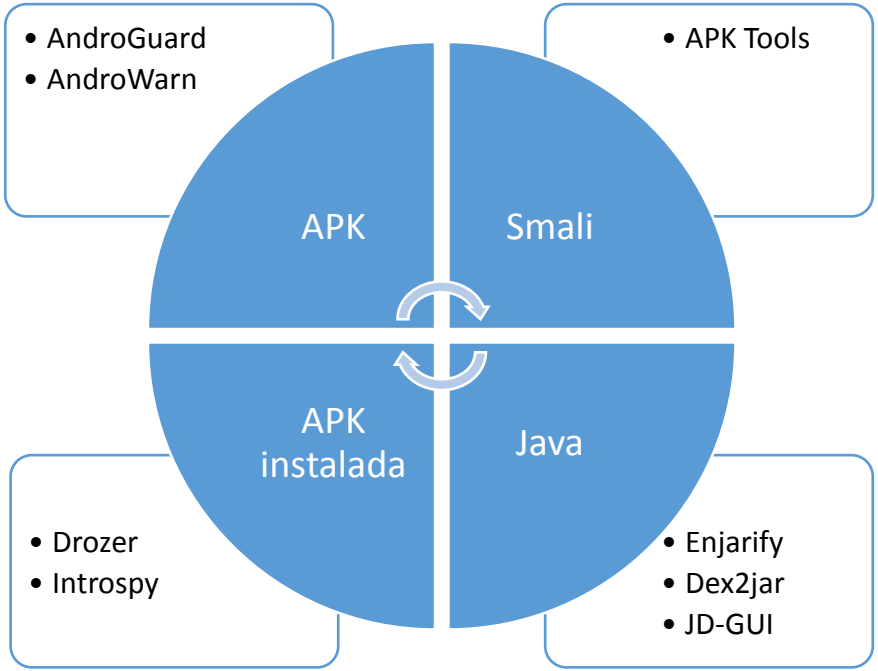
¿Qué?

Posibles problemas de seguridad

Security Issue	Description
Authentication	Issues related to user identification
Access Control	Issues related to user rights after authentication
Auditing and Logging	Issues related to logs and auditing
Cryptography	Issues related to encryption and securing communications
Credential Handling	Issues related to the handling of user passwords and other credentials
Data Handling	Issues related to the handling of data vis-à-vis its sensitivity
Data Leakage	Issues related to accidental or unintended leakage of information
Error Checking	Issues related to reporting errors without providing too much data
Input Validation	Issues related to validating untrusted user input
Session Management	Issues related to best practices for user session management
Resource Handling	Issues related to the handling of resources, including memory
Patching	Issues related to timely patching/upgrade of software

Tipos de herramientas

Vista previa



Tipos de herramientas

Tipologías de herramientas necesarias

- Análisis Estático
- Análisis Dinámico
- Reversing

Herramientas Análisis Estático

AndroGuard

```
root@AndroidKali:~/Herramientas/androguard# ./androlyze.py -s
Androlyze version 2.0
In [1]: a,d,dx = AnalyzeAPK("HolaMundo.apk", decompiler="dad")

In [2]: a.get_permissions()
Out[2]:
['android.permission.SEND_SMS',
 'android.permission.READ_SMS',
 'android.permission.RECEIVE_SMS',
 'android.permission.READ_PHONE_STATE',
 'android.permission.READ_CONTACTS']
```

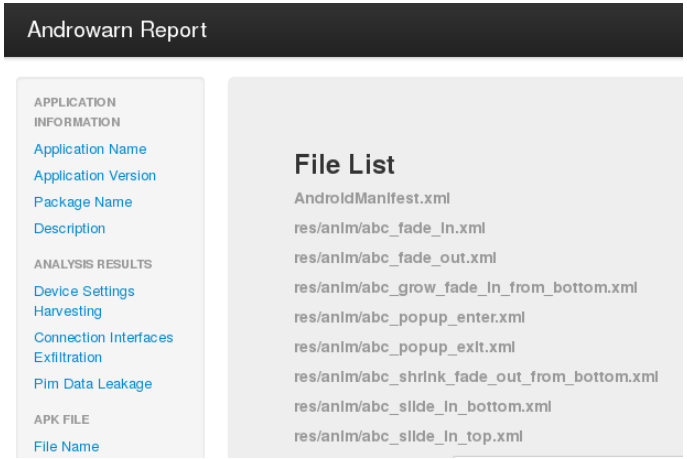
```
In [30]: a.get_permissions()
Out[30]:
['android.permission.INTERNET',
 'android.permission.ACCESS_WIFI_STATE',
 'android.permission.CHANGE_WIFI_STATE',
 'android.permission.ACCESS_NETWORK_STATE',
 'android.permission.ACCESS_COURSE_LOCATION',
 'android.permission.ACCESS_FINE_LOCATION',
 'android.permission.READ_PHONE_STATE',
 'android.permission.SEND_SMS',
 'android.permission.RECEIVE_SMS',
 'android.permission.RECORD_AUDIO',
 'android.permission.CALL_PHONE',
 'android.permission.READ_CONTACTS',
 'android.permission.WRITE_CONTACTS',
 'android.permission.RECORD_AUDIO',
 'android.permission.WRITE_SETTINGS',
 'android.permission.CAMERA',
 'android.permission.READ_SMS',
 'android.permission.WRITE_EXTERNAL_STORAGE']
```

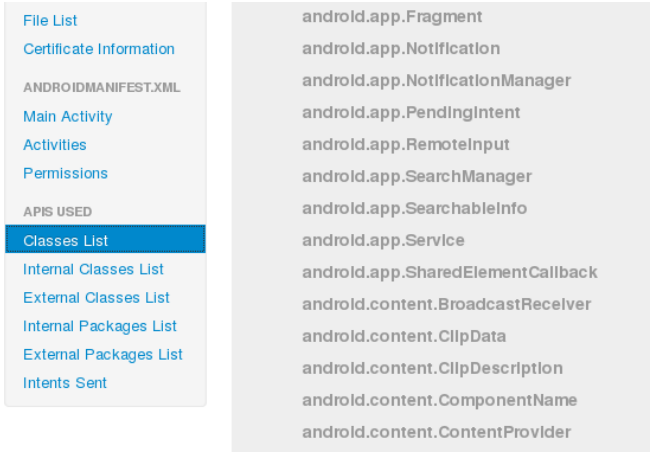
Herramientas Análisis Estático

AndroWarn

- Basado en AndroGuard

```
root@AndroidKali:~/Herramientas/Androwarn# python androwarn.py -i HolaMundo.apk -r html
 -v 3
[+] Analysis successfully completed and HTML file report available './Report/com.exampl
e.mirojo.holamundo.html'
```





Tipos de herramientas

Tipologías de herramientas necesarias

- Análisis Estático
- Análisis Dinámico
- Reversing

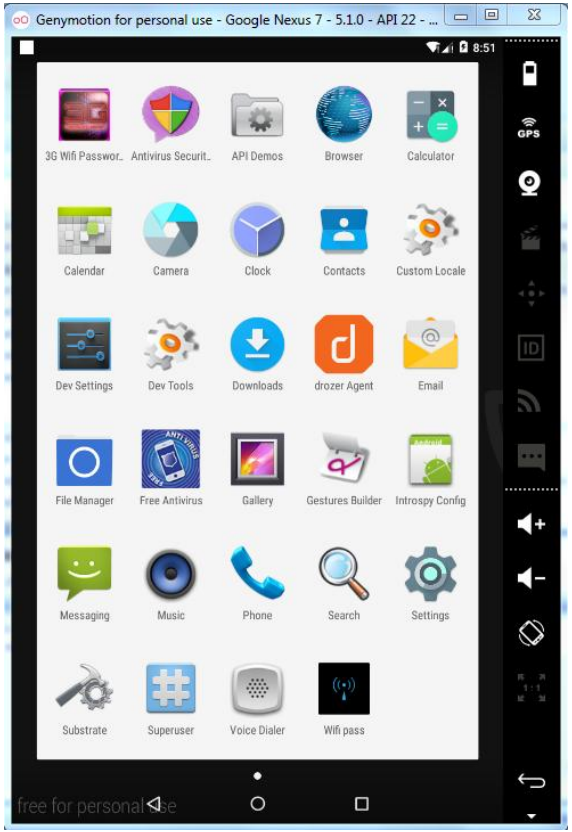
Herramientas Análisis Dinámico

Drozer

```
C:\Program Files\drozer>drozer console connect
Selecting 34b085acb18fedd6 (Genymotion Google Nexus 7 - 5.1.0 - API 22 - 800x128
0 5.1)

                ..                    ..:.
              ..o..                   .r..
               ..a..  . ....... .  ..nd
                 ro..idsnemesisand..pr
                   .otectorandroidsneme.
               .,sisandprotectorandroids+.
             ..nemesisandprotectorandroidsn:.
           .emesisandprotectorandroidsnemes..
         ..isandp,...,rotectorandro,...,idsnem.
        .isisandp..rotectorandroid..snemisis.
        .andprotectorandroidsnemisisandprotec.
       .torandroidsnemesisandprotectorandroid.
       .snemisisandprotectorandroidsnemesisan:
       .dprotectorandroidsnemesisandprotector.

drozer Console (v2.3.4)
dz>
```

```
dz> run app.package.list
com.example.android.livecubes (Example Wallpapers)
com.android.providers.telephony (Mobile Network Configuration)
com.android.providers.calendar (Calendar Storage)
com.android.providers.media (Media Storage)
com.android.wallpapercropper (com.android.wallpapercropper)
ss.passion.blockgram (Free Antivirus)
com.android.voicedialer (Voice Dialer)
com.android.documentsui (Documents)
com.android.galaxy4 (Black Hole)
```

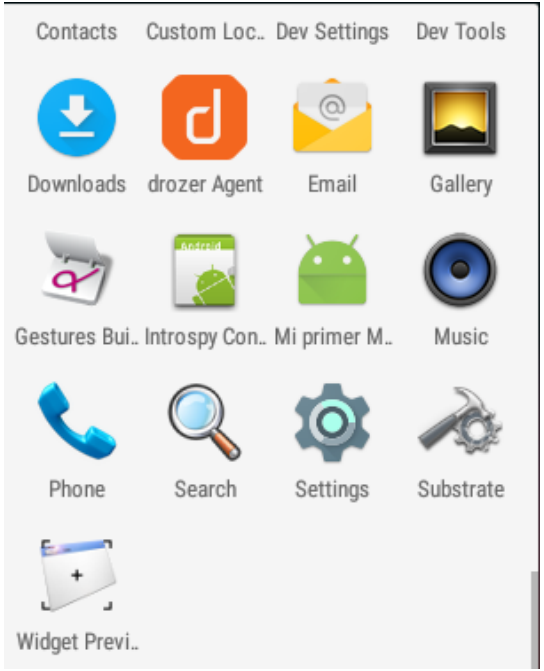
```
dz> list
app.activity.forintent      Find activities that can handle the given intent

app.activity.info           Gets information about exported activities.

app.activity.start          Start an Activity

app.broadcast.info          Get information about broadcast receivers

app.broadcast.send          Send broadcast using an intent
```



Herramientas Análisis Dinámico

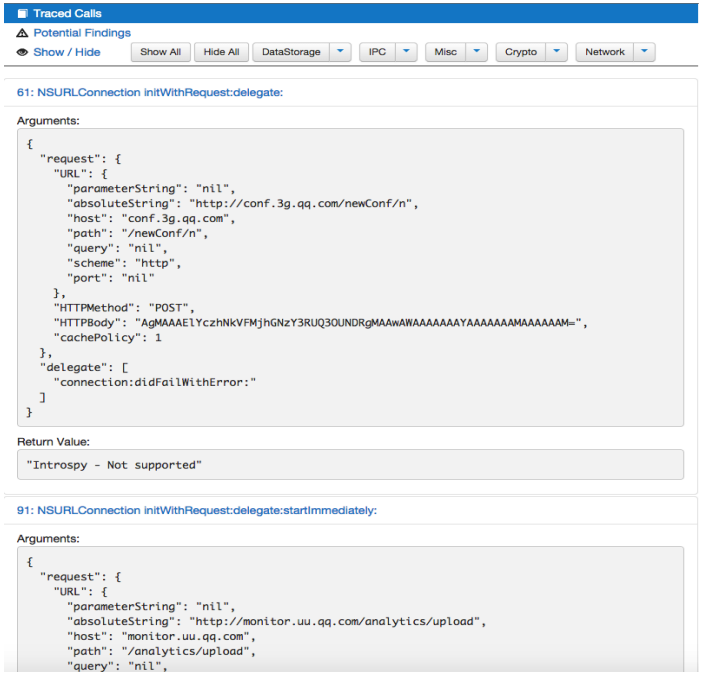
Introspy

```
D:\Android\sdk\platform-tools>adb install "Introspy-Android Config.apk"
887 KB/s (20915 bytes in 0.023s)
        pkg: /data/local/tmp/Introspy-Android Config.apk
Success

D:\Android\sdk\platform-tools>adb install "Introspy-Android Core.apk"
984 KB/s (241983 bytes in 0.240s)
        pkg: /data/local/tmp/Introspy-Android Core.apk
Success

D:\Android\sdk\platform-tools>adb install com.saurik.substrate.apk
995 KB/s (1573498 bytes in 1.544s)
        pkg: /data/local/tmp/com.saurik.substrate.apk
Success

D:\Android\sdk\platform-tools>adb logcat -s "Introspy"
--------- beginning of main
--------- beginning of system
--------- beginning of crash
```



Herramientas Análisis Dinámico

Introspy



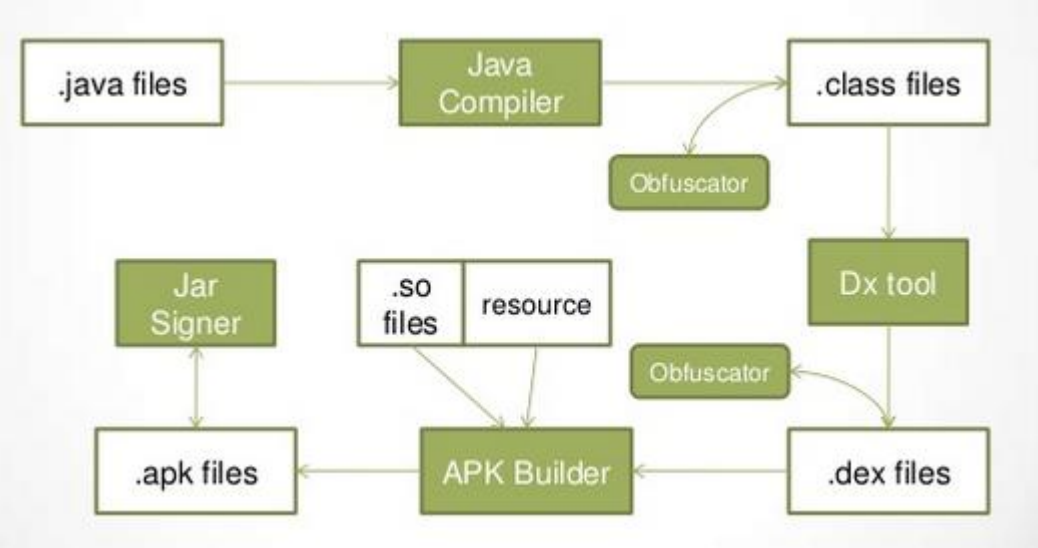
Tipos de herramientas

Tipologías de herramientas necesarias

- Análisis Estático
- Análisis Dinámico
- Reversing

Herramientas Reversing

Ciclo de reversing para archivos java



Herramientas Reversing

Enjarify o dex2jar

```
D:\Android\dex2jar>d2j-dex2jar fbi.apk
dex2jar fbi.apk -> .\fbi-dex2jar.jar
```

```
D:\Android\enjarify\enjarify-master>enjarify.bat fbi.apk
1000 classes processed
Output written to fbi-enjarify.jar
1115 classes translated successfully, 0 classes had errors
```

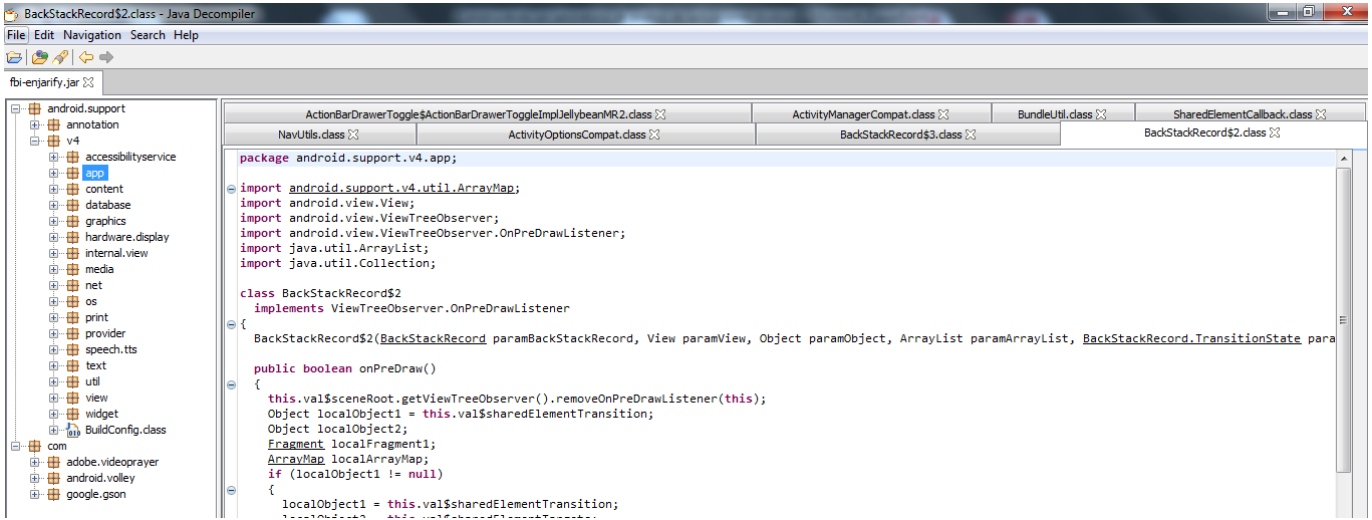
fbi-dex2jar	18/11/2015 11:12	Executable Jar File	1.100 KB
fbi-enjarify	18/11/2015 11:08	Executable Jar File	1.766 KB

Why not dex2jar?

Dex2jar is an older tool that also tries to translate Dalvik to Java bytecode. It works reasonable well most of the time, but a lot of obscure features or edge cases will cause it to fail or even silently produce incorrect results. By contrast, Enjarify is designed to work in as many cases as possible, even for code where Dex2jar would fail. Among other things, Enjarify correctly handles unicode class names, constants used as multiple types, implicit casts, exception handlers jumping into normal control flow, classes that reference too many constants, very long methods, exception handlers after a catchall handler, and static initial values of the wrong type.

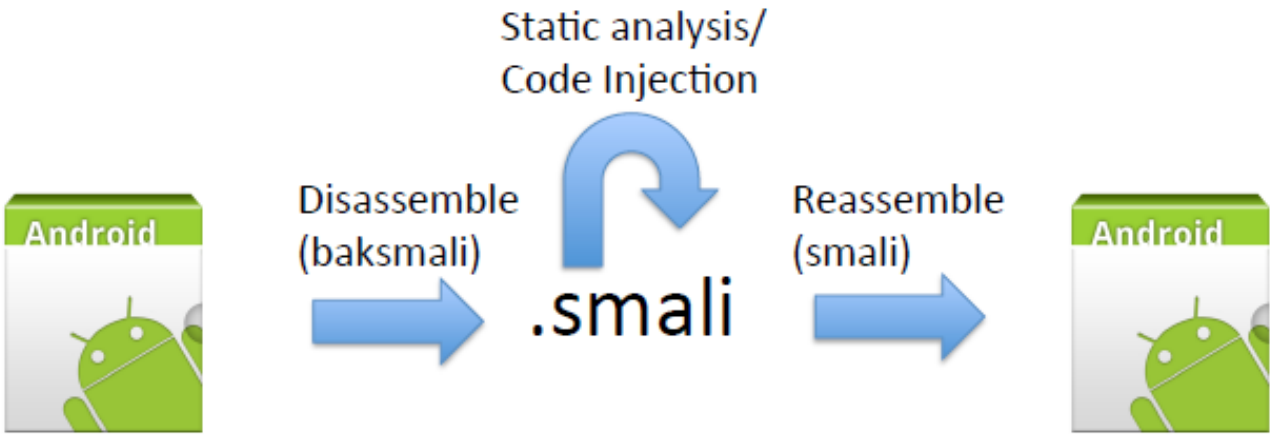
Herramientas Reversing

JD-GUI



Herramientas Reversing

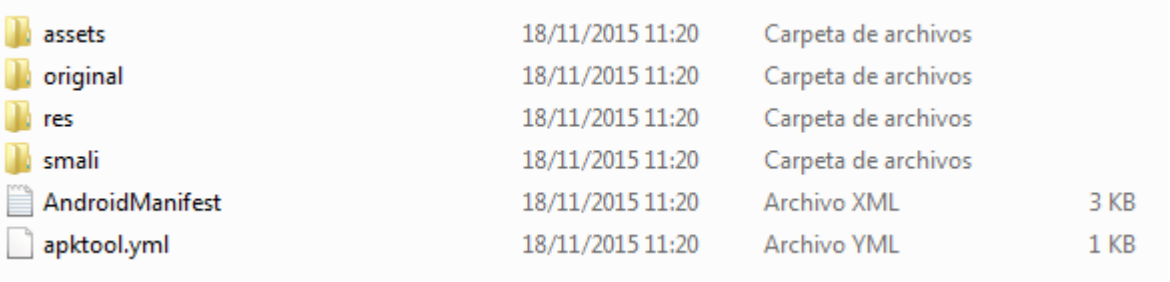
Ciclo de reversing para archivos smali



Herramientas Reversing

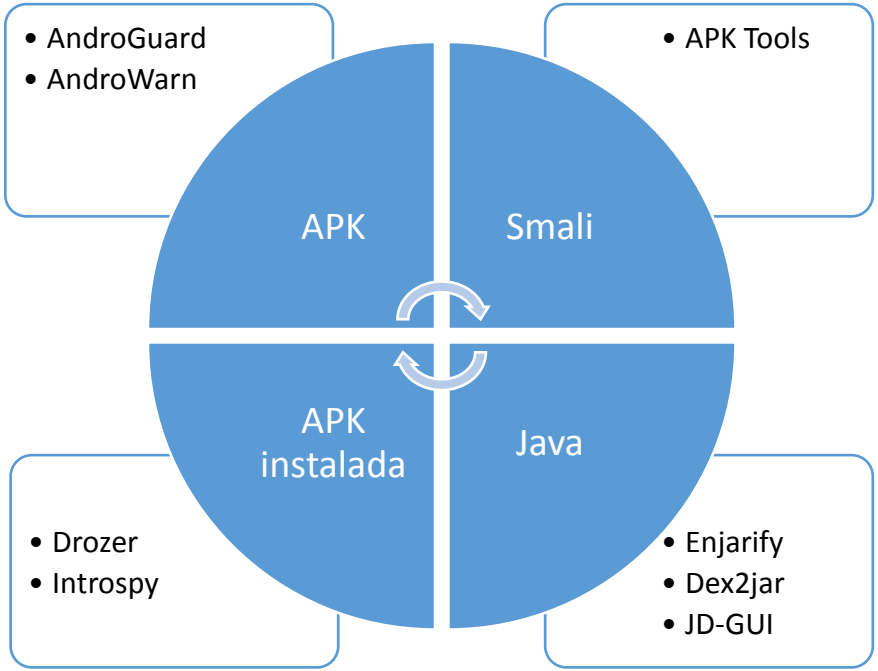
APKTool

```
D:\Android\APKTool202>apktool_202.jar d fbi.apk
```



Tipos de herramientas

Resumen



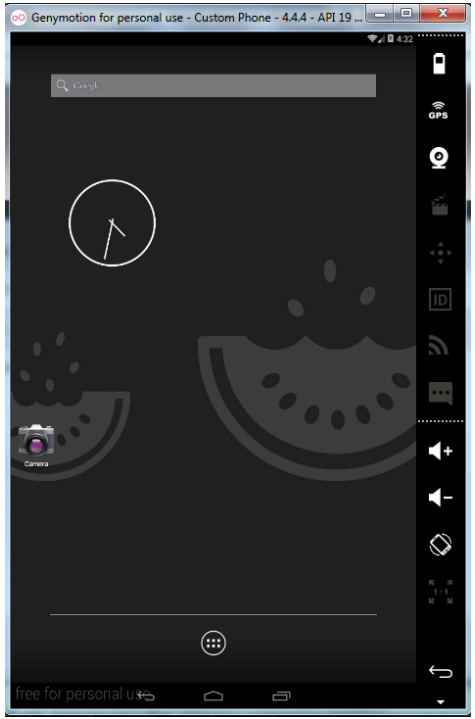
Otras Herramientas

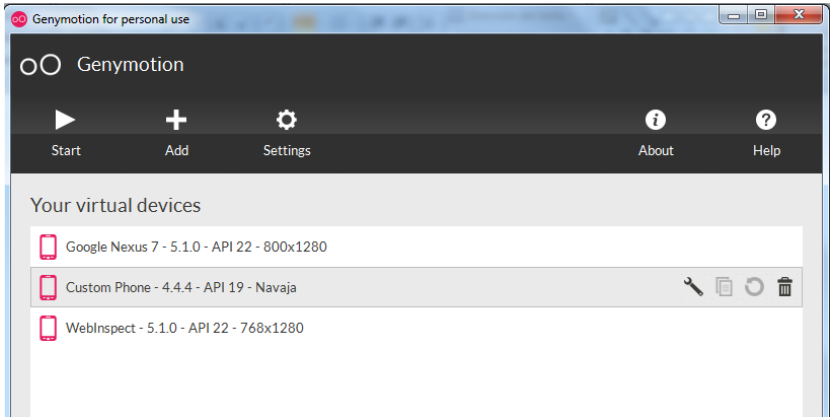
Otras herramientas de interés

- Genymotion
- Burp Proxy
- WireShark
- Android Studio
  - Lint
- Agnitio

Otras Herramientas

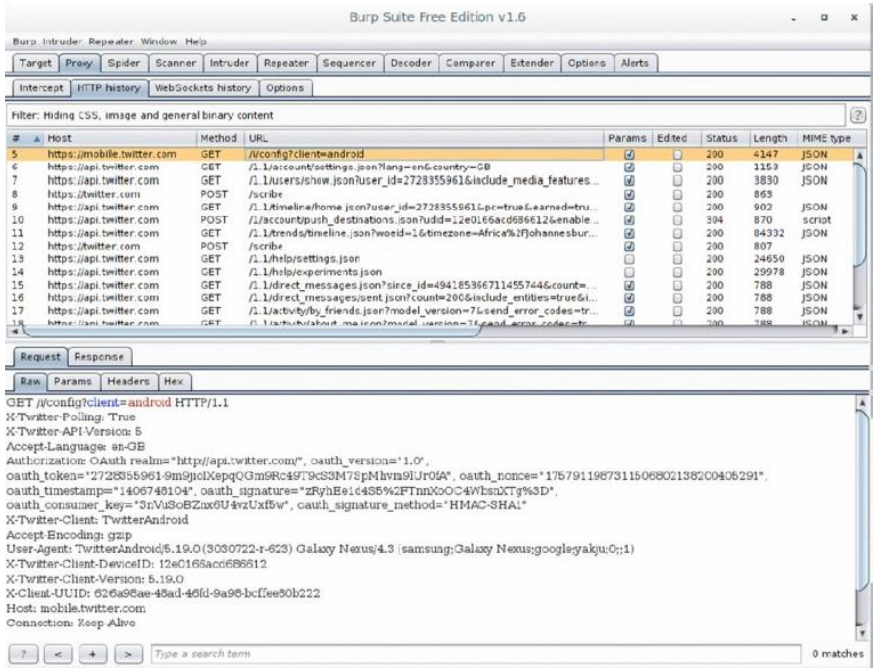
Otras herramientas de interés. Genymotion

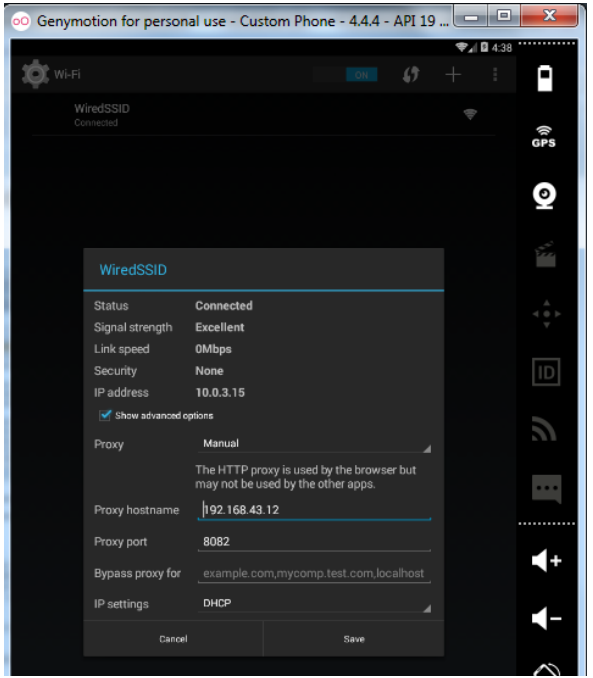




Otras Herramientas

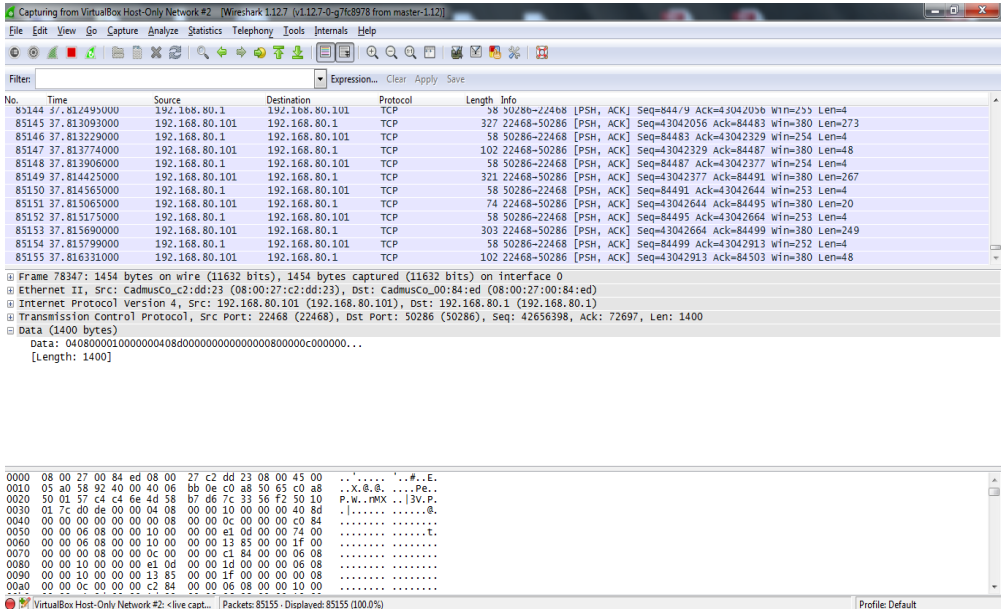
Otras herramientas de interés. Burp Proxy





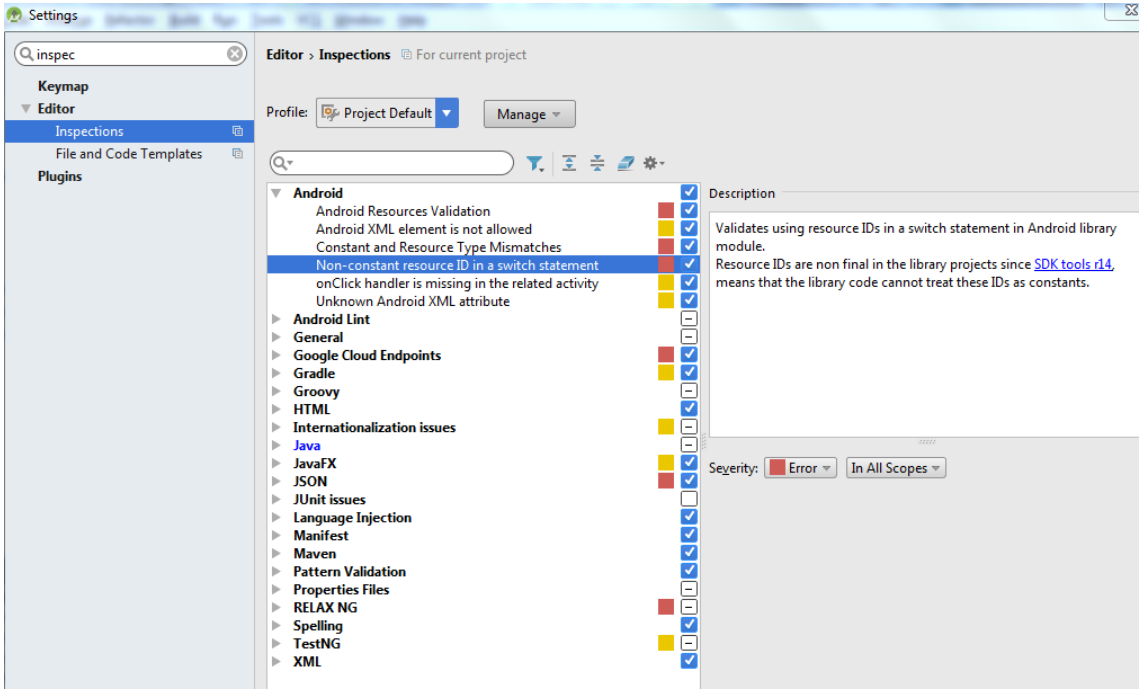
Otras Herramientas

Otras herramientas de interés. WireShark



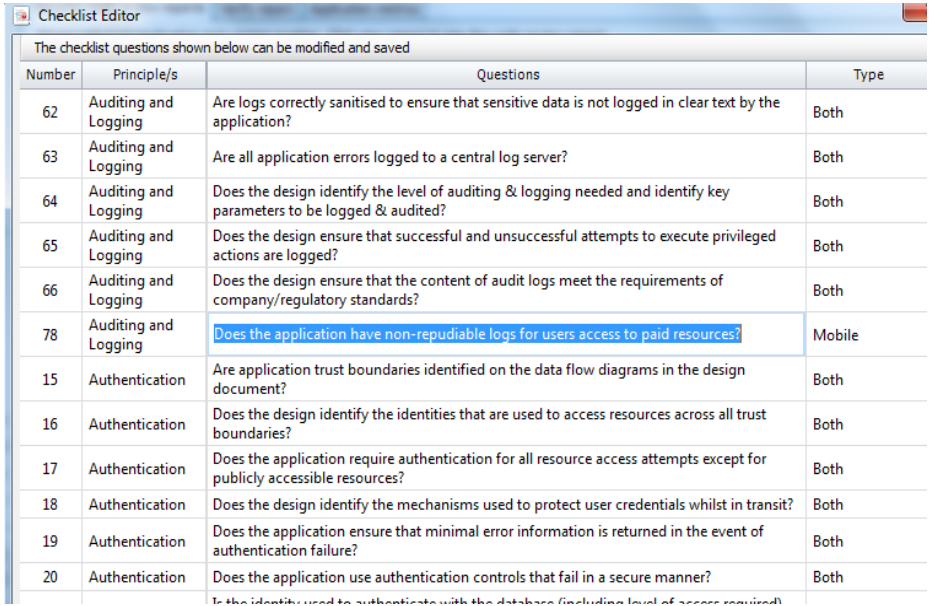
Otras Herramientas

Otras herramientas de interés. Lint



Otras Herramientas

Otras herramientas de interés. Agnitio



Checklist Editor

The checklist questions shown below can be modified and saved

Number	Principle/s	Questions	Type
62	Auditing and Logging	Are logs correctly sanitised to ensure that sensitive data is not logged in clear text by the application?	Both
63	Auditing and Logging	Are all application errors logged to a central log server?	Both
64	Auditing and Logging	Does the design identify the level of auditing & logging needed and identify key parameters to be logged & audited?	Both
65	Auditing and Logging	Does the design ensure that successful and unsuccessful attempts to execute privileged actions are logged?	Both
66	Auditing and Logging	Does the design ensure that the content of audit logs meet the requirements of company/regulatory standards?	Both
78	Auditing and Logging	Does the application have non-repudiable logs for users access to paid resources?	Mobile
15	Authentication	Are application trust boundaries identified on the data flow diagrams in the design document?	Both
16	Authentication	Does the design identify the identities that are used to access resources across all trust boundaries?	Both
17	Authentication	Does the application require authentication for all resource access attempts except for publicly accessible resources?	Both
18	Authentication	Does the design identify the mechanisms used to protect user credentials whilst in transit?	Both
19	Authentication	Does the application ensure that minimal error information is returned in the event of authentication failure?	Both
20	Authentication	Does the application use authentication controls that fail in a secure manner?	Both

Distribuciones

Distribuciones especializadas en Android

- Appie – 02/2015 https://manifestsecurity.com/appie/
- Santoku – 2014 https://santoku-linux.com/
- MobiSec – 05/2015 http://mobisec.professionallyevil.com/
- Vezir – 06/2015 https://github.com/oguzhantopgul/Vezir-Project

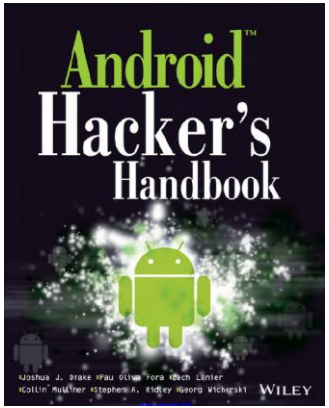
Referencias

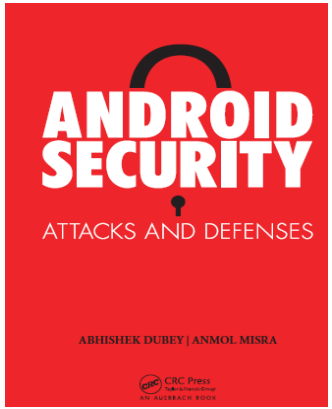
Herramientas

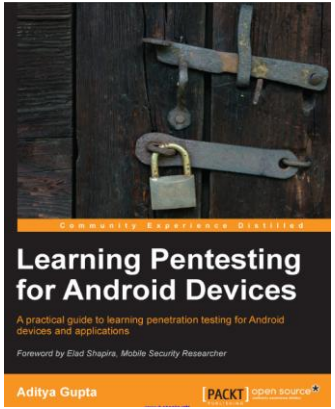
- APKTool http://ibotpeaches.github.io/Apktool/
- Enjarify https://github.com/google/enjarify
- Dex2Jar https://github.com/pxb1988/dex2jar
- JD-GUI http://jd.benow.ca/
- AndroGuard https://github.com/androguard/androguard
- Androwarn https://github.com/maaaaz/androwarn
- Introspy https://github.com/iSECPartners/Introspy-Android
- Drozer https://www.mwrinfosecurity.com/products/drozer/

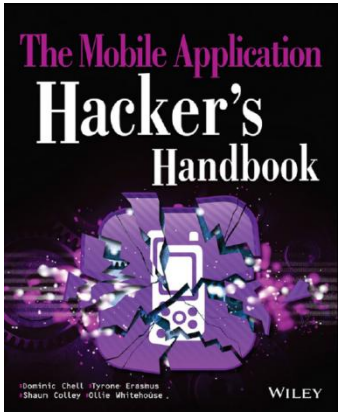
Referencias

Referencias









https://koodous.com

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en Linked in