

Pentest Mobile

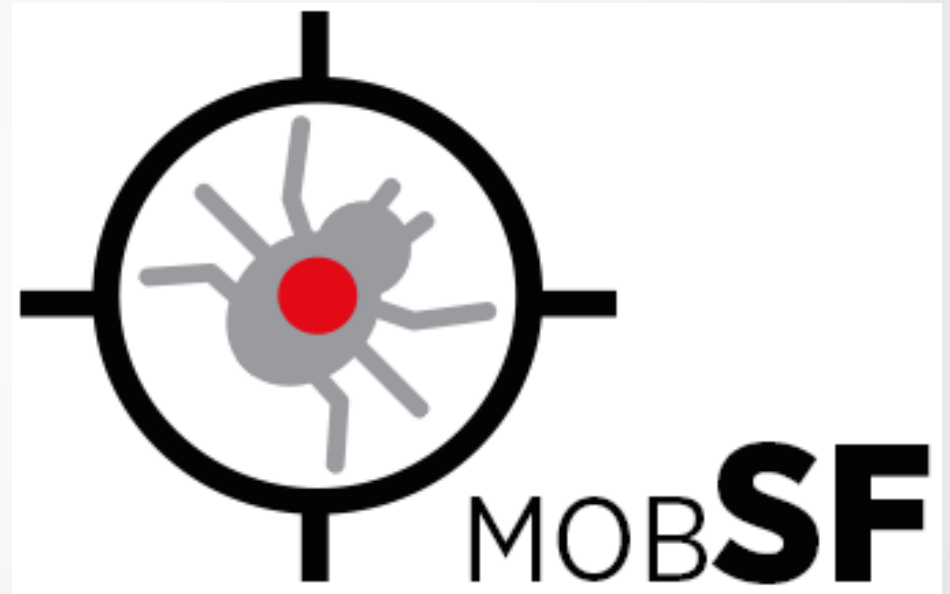


Android x IOS

- Dispositivo (# ou \$)
- ADB
- AVD, Genymotion
- Smali
- Proxy (Burp)
- Jailbreak
- Cydia
- Keychain
- Xcode
- Proxy (Charles Proxy)

Mobile Security Framework (MobSF)

- Scanner
- Análise estática (APK, IPA)
- Relatório de vulnerabilidades
- Análise dinâmica Android (Frida)



MobSF

MobSF

Static Analysis

Information

Scan Options

Signer Certificate

Permissions

Binary Analysis

Android API

Browsable Activities

Security Analysis

Malware Analysis

Reconnaissance

Components

Download Report

Dynamic Analysis Report

Recent Scans

API Docs

About

Search MDS

Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	Dangerous	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	Dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.DELETE_PACKAGES	SignatureOrSystem	delete applications	Allows an application to delete Android packages. Malicious applications can use this to delete important applications.
android.permission.GET_TASKS	Dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.ACCESS_NETWORK_STATE	Normal	view network status	Allows an application to view the status of all networks.
com.android.launcher.permission.INSTALL_SHORTCUT	Dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.READ_PHONE_STATE	Dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
com.google.android.providers.gsf.permission.READ_GSERVICES	Dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	Dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

OWASP Mobile top 10



- www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main
- www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Android Debug Bridge (ADB)

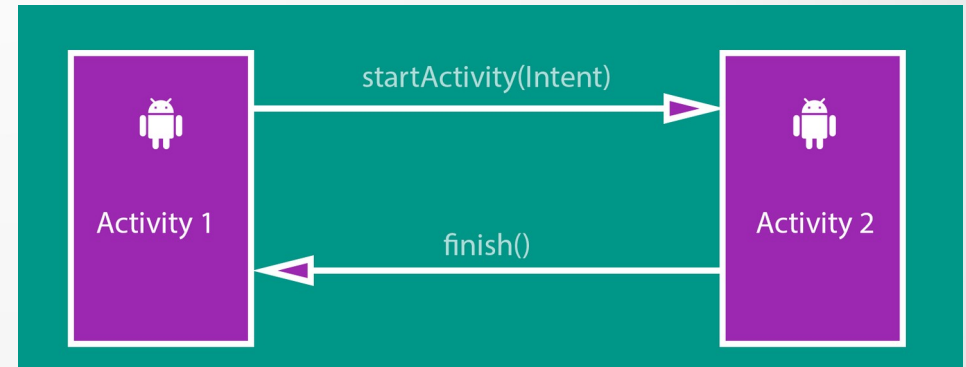
- Ponte de comunicação entre o terminal e o dispositivo móvel.
- Instala e desinstala APKs
- Comandos Shell
- Copia e envia arquivos para o dispositivo



PM / AM

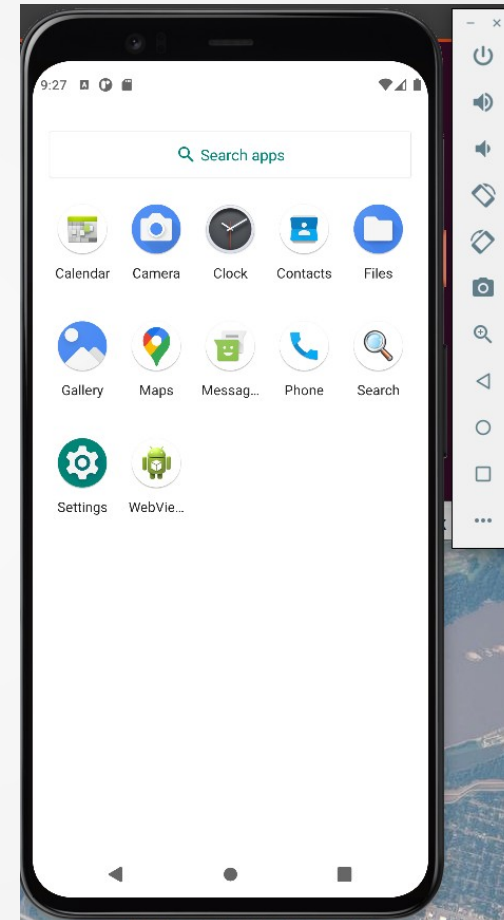
- Package Manager
- Listar pacotes
- Desinstalar pacotes
- Activity Manager
- Inicia/para uma atividade
- Envia Broadcast

```
platform-tools -- bash -- 99x19
~/canary_fresh_sdk/platform-tools -- bash
lgleaseon@MacBook-Pro-40:~/canary_fresh_sdk/platform-tools$ ./adb shell pm list packages
package:com.android.cts.priv.ctsshim
package:com.google.android.ext.services
package:com.android.providers.telephony
package:com.android.providers.calendar
package:com.android.providers.media
package:com.google.android.ext.shared
package:com.android.iotlauncher.ota
package:com.android.documentsui
package:com.android.externalstorage
package:com.android.htmlviewer
package:com.android.companiondevicemanager
package:com.android.providers.downloads
package:com.google.android.things.internal.media
package:com.google.android.iot.frameworkpackagestubs
package:com.android.defcontainer
package:com.android.pacprocessor
package:com.google.wifisetup
package:com.android.certinstaller
```



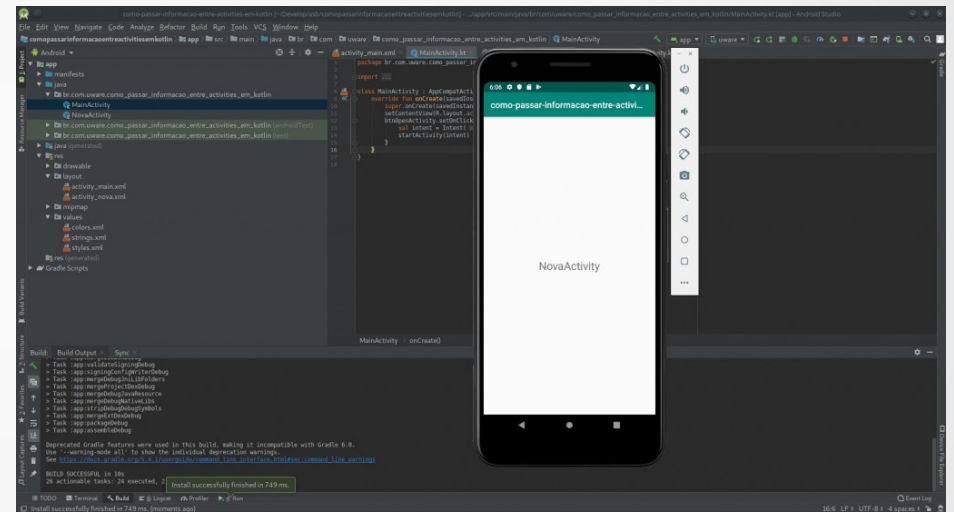
AVD (Android Virtual Device)

- Ambiente virtual que emula um dispositivo físico
- Fácil execução pelo Emulator (Executa uma AVD)
- Escolha entre versões Android (incluindo PlayStore)



Android Studio

- Ambiente de desenvolvimento Android
- Inclui (ADB, AVD entre outros)
- Debug



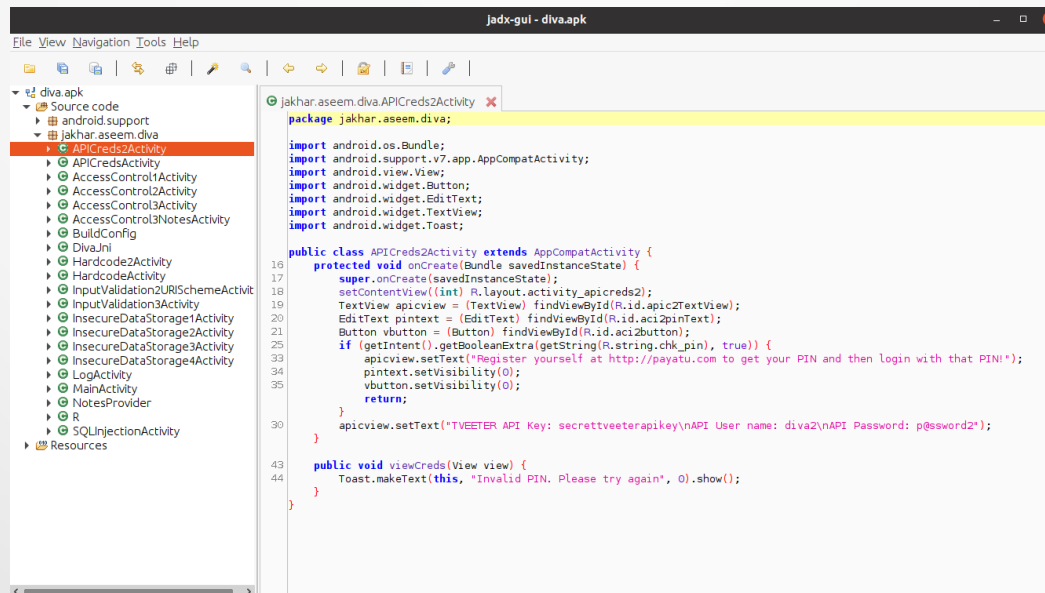
APKTool

- Engenharia reversa
- Compila / Descompila APKs

```
~/Android/Android-Pentest via ☕ v1.8.0  
> java -jar apktool.jar d ~/Downloads/diva.apk  
I: Using Apktool 2.3.3 on diva.apk  
I: Loading resource table...  
I: Decoding AndroidManifest.xml with resources...  
S: WARNING: Could not write to (/home/tsalmeida/.local/share/apktool/fra  
S: Please be aware this is a volatile directory and frameworks could go  
I: Loading resource table from file: /tmp/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...
```

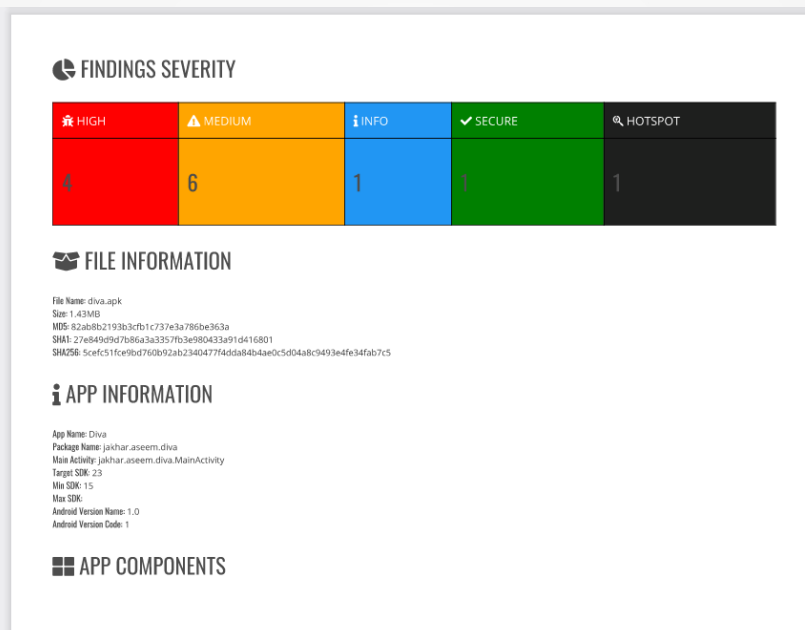
JADX e JDGui

- Engenharia reversa
- Dex2Jar
- Código + compreensível (em Java)
- Contém GUI (Interface gráfica)



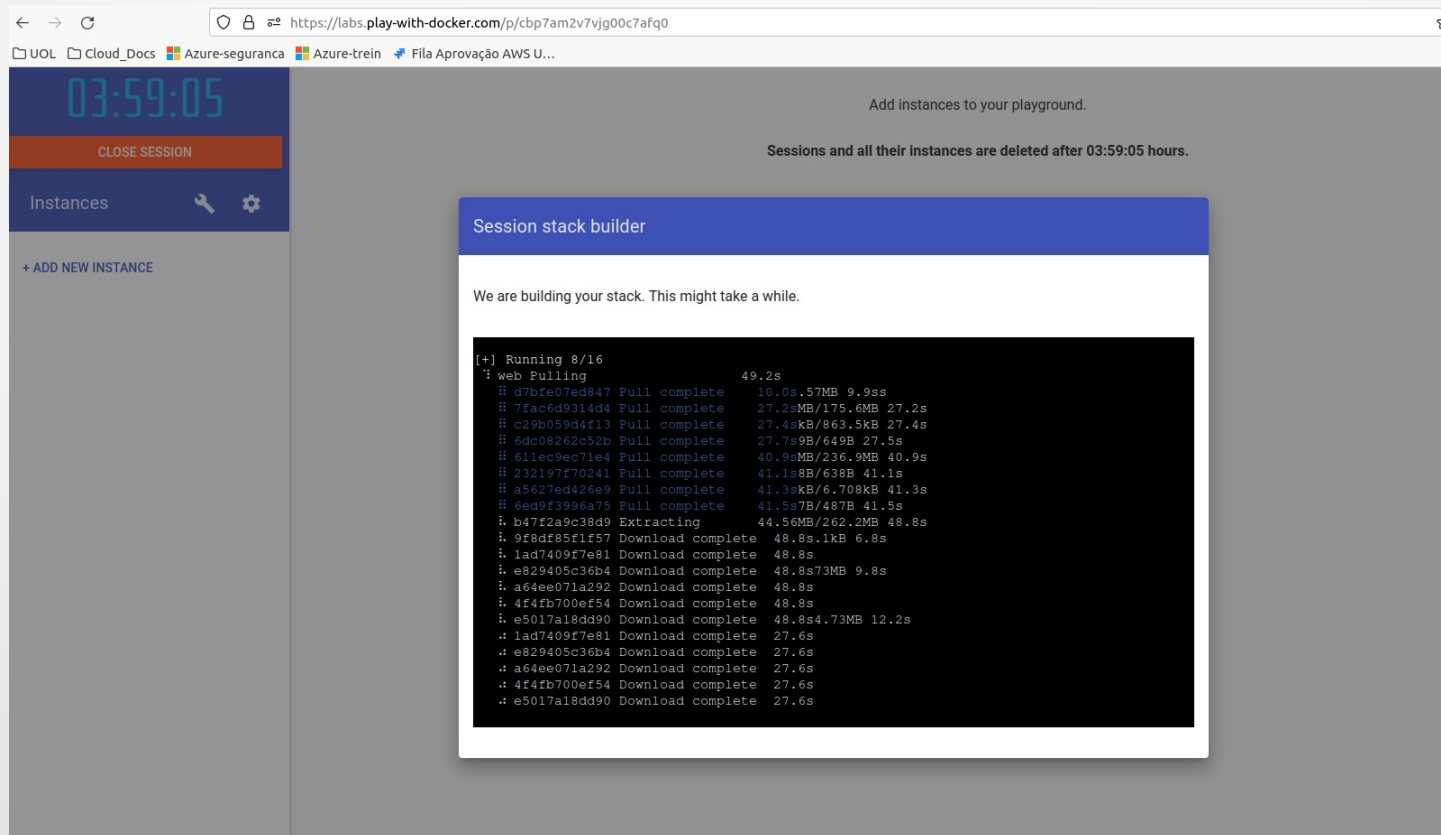
Instalação MobSF

- Instalação local (setup.sh, setup.bat)
- Via Docker Image (não executa análise dinâmica)



MobSF sem instalação

- PlayWithDocker
- Direto navegador

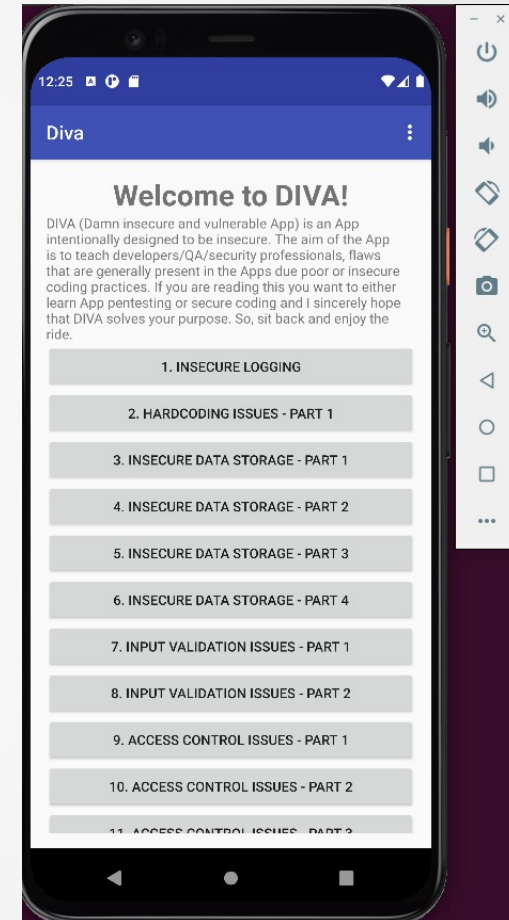


DIVA

- Damn insecure and vulnerable app
- Exploração de falhas

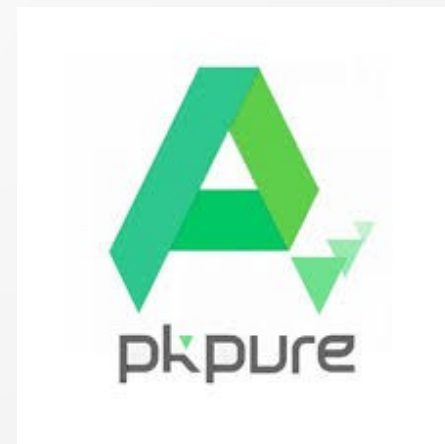
Outros APPs:

- GoatDroid
- Fourgoats



Baixando APPs

- APK Downloader
- Direto GooglePlay
- APKpure
- Baixar versões + antigas



Fim

Obrigado!

