EJERCICIOS ANÁLISIS Y GENERACIÓN DE INFORMES

PREREQUISITOS

- KALI LINUX
- ANDROID

Ejercicio 1 – MobSF

- Análisis estático y generación de informe de la aplicación que elijas utilizando MobSF

```
┌──(root㉿kali)-[/home/veronica/Descargas/InsecureBankv2/dist]
└─# adb connect 192.168.100.78:5555
already connected to 192.168.100.78:5555
```

```
┌──(root㉿kali)-[/home/veronica/Descargas]
└─# adb install warp.apk
Performing Streamed Install
Success
```

La app analizada es una app editor de fotografías y videos., filtros etc para tiktok.

Los informes de análisis de estáticos son:

- Warp.pdf
- Static análisis.pdf
- Appsec scorecard.pdf

Realizamos un pequeño análisis de los resultados que son muy completos,

APP INFORMATION

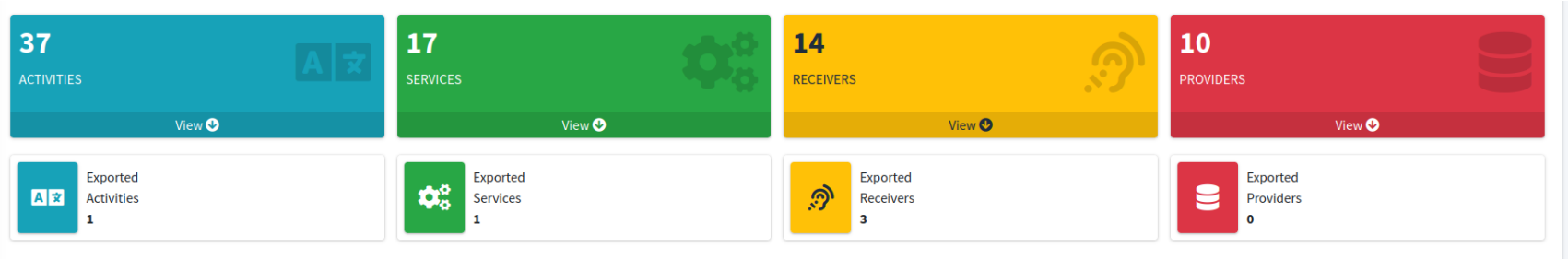
App Name Time Warp
Package Name com.timewarp.scan.bluelinefiltertiktok.free
Main Activity com.timewarp.scan.bluelinefiltertiktok.free.MainActivity
Target SDK 30 Min SDK 24 Max SDK
Android Version Name 2.10 Android Version Code 27

Vemos la información de la app el nombre del paquete y main activity, el target SDK que es la API con que la aplicación esta compilada.

Abajo vemos el nombre de la aplicación , url playstore, entre otras informaciones generales.

Title Time Warp Scan - Face Scanner
Score 3.7358916 **Installs** 10,000,000+ **Price** 0 **Android Version Support** **Category** Photography **Play Store URL** com.timewarp.scan.bluelinefiltertiktok.free
Developer Braly Co., Ltd, **Developer ID** 6509386962817851798
Developer Address 31 Dich Vong Street - Cau Giay - Ha Noi - Viet Nam
Developer Website https://istore68.blogspot.com/ads.txt
Developer Email cameraselfie.store@gmail.com
Release Date Mar 4, 2022 **Privacy Policy** Privacy link
Description

Abajo se ve las actividades, servicios, recivers y providers,



La app se encuentra firmada, el v1 es false por lo que el firmante no firmo la app tradicionalmente las otras dos firmas si son true por lo que se realizaron de manera estándar.

SIGNER CERTIFICATE

```
APK is signed
v1 signature: False
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-03-04 16:10:27+00:00
Valid To: 2052-03-04 16:10:27+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x50c0b71ae6b6277e5b7c9fe80d6a0b2779c176b3
Hash Algorithm: sha256
md5: 6fee4d992984f10b8c8bcafa82a44f4d
sha1: 01ff7258eeccaf7a89f9588035a01d7c4dbb3cdd
sha256: d2479b2f33206c7a62aaf675935c75510d39eef668e0f4b253ff4f8c6c0ac980
sha512: c69629fac176b044b0f7211d14df69faedd1e5dd94be2e0ae7f60e8d54b51f2cb626bf7cb6634aabc9378673c33d53665ab5f020a7cda4224f44f39bc570ebf8
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 6676513a065a5cfd8808f8349208829221e6609201e0751036533bf80c818074
```

En cuanto a los permisos podemos ver que uno peligroso detectado es el permiso que se le da a la app para almacenar nuestras imágenes y pueden ser vistas en cualquier momento. Otra es que la aplicación reconoce la ruta de los audios realizados, y la ultima que la aplicación puede acceder al almacenamiento externo.

android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

En cuanto a la red, tiene dos vulnerabilidades severas, detecto que la red esta configurada inseguramente y esto permite el rastreo del trafico a todos los dominios.

NETWORK SECURITY

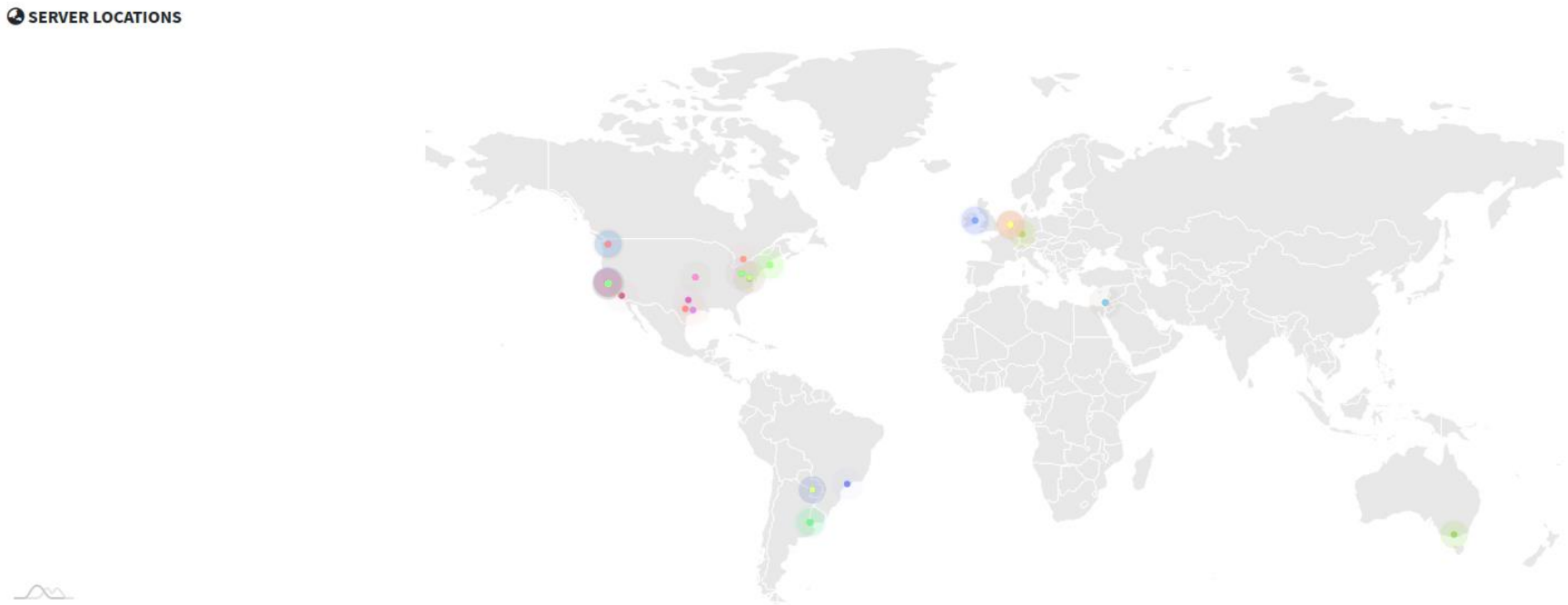
NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	127.0.0.1	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

En cuanto al código, existen vulnerabilidades como insertan información sensible en un archivo log, se detecto el uso de algoritmo criptografico riesgoso, la dirección IP esta expuesta, hay unos errores de permisos.

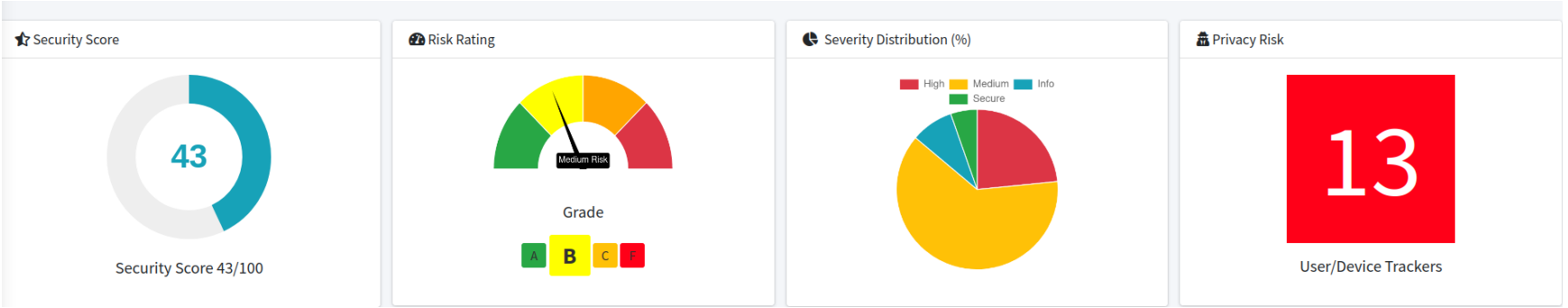
En cuanto a las librerías utilizadas en el informe se puede visualizar que hay muchos warnings como que el objeto compartido no posee funciones fortificadas.

EL NIAP análisis básicamente detecto que se utiliza llaves asimétricas, que la aplicación tiene acceso a la red, fotografías, videos y audios.

Podemos ver también la localización de los servidores.



El puntaje de seguridad es de 43/100 lo cual significa que la aplicación tiene vulnerabilidades.



La mayoría de las vulnerabilidades son de riesgo medio y el rating esta en grado B.

Algunas de las vulnerabilidades mas severas son primero, los dominios y el base config están configurados inseguramente, la implementación del SSL es insegura, por lo que es vulnerable a ataques MITM, el modo depuración de la aplicación esta activado, la aplicación contiene rastreador de privacidad.

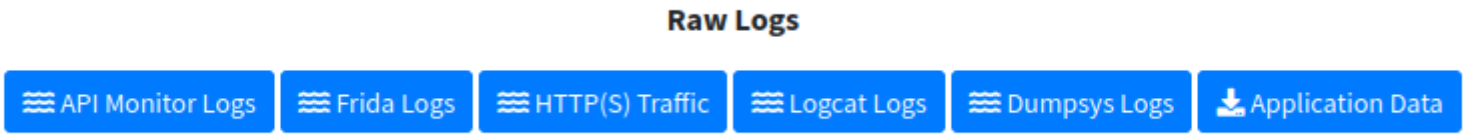
Cabe resaltar que la aplicación detecta al root de otros usuarios.

Las informaciones mas completas se encuentran en los reportes.

Ejercicio 2 - MobSF y Android

- Análisis dinámico y generación de informe de la aplicación que elijas utilizando MobSF

En cuanto al análisis dinamico podemos ver información de la aplicación de manera dinámica, es decir la app en movimiento, abajo vemos los ítems que podemos examinar.



Por ejemplo, en el ítem de FRIDA logs después de realizar algunos movimientos dentro de la aplicación podemos ver lo que ha detectado parcialmente.

Podemos ver que ha detectado al root luego de que haya navegado a través de la Shell en por los directorios, aplicaciones, configuraciones, etc.

Exploramos HTTPS traffic y trae un request y response parecido a lo que captura burpsuite,

En Logcat logs se visualiza el proceso de creación de la app, su evolución desde el 2017 cuando se creo hasta sus ultimas actualizaciones.

En dumpsys logs se visualizan los servicios que actualmente utiliza la app como ser audio, alarma , adb, etc.

En el archivo application data se encuentran metadatos de la aplicación que son bastante pesados por ende no lo descarge.

```
Loaded Frida Script - root_bypass
Loaded Frida Script - api_monitor
Loaded Frida Script - debugger_check_bypass
Loaded Frida Script - ssl_pinning_bypass
[RootDetection Bypass] test-keys check
[RootDetection Bypass] return value for binary: Superuser.apk
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] test-keys check
[RootDetection Bypass] return value for binary: Superuser.apk
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] test-keys check
[RootDetection Bypass] test-keys check
[RootDetection Bypass] return value for binary: Superuser.apk
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] test-keys check
[RootDetection Bypass] return value for binary: Superuser.apk
[RootDetection Bypass] return value for binary: su
[API Monitor] Cannot find org.apache.http.impl.client.AbstractHttpClient.exe
[API Monitor] Cannot find com.android.okhttp.internal.http.HttpURLConnectior
[SSL Pinning Bypass] okhttp CertificatePinner not found
[SSL Pinning Bypass] okhttp3 CertificatePinner not found
[SSL Pinning Bypass] DataTheorem trustkit not found
[SSL Pinning Bypass] Appcelerator PinningTrustManager not found
[SSL Pinning Bypass] Apache Cordova SSLCertificateChecker not found
[SSL Pinning Bypass] Wultra CertStore.validateFingerprint not found
[SSL Pinning Bypass] Xutils not found
[SSL Pinning Bypass] httpclientandroidlib not found
[SSL Pinning Bypass] Cronet not found
[SSL Pinning Bypass] certificatetransparency.CTInterceptorBuilder not found
[RootDetection Bypass] root check for package: com.noshufou.android.su
[RootDetection Bypass] root check for package: com.noshufou.android.su.elite
[RootDetection Bypass] root check for package: eu.chainfire.supersu
[RootDetection Bypass] root check for package: com.koushikdutta.superuser
[RootDetection Bypass] root check for package: com.thirdparty.superuser
[SSL Pinning Bypass] checkTrustedRecursive() bypassed
[RootDetection Bypass] root check for package: com.yellowes.su
[SSL Pinning Bypass] checkTrustedRecursive() bypassed
[SSL Pinning Bypass] checkTrustedRecursive() bypassed
[RootDetection Bypass] root check for package: com.koushikdutta.rommanager
[RootDetection Bypass] root check for package: com.koushikdutta.rommanager.l
[SSL Pinning Bypass] checkTrustedRecursive() bypassed
[RootDetection Bypass] root check for package: com.dimonvideo.luckypatcher
[RootDetection Bypass] root check for package: com.chelpus.lackypatch
[RootDetection Bypass] root check for package: com.ramdroid.appquarantine
[SSL Pinning Bypass] checkTrustedRecursive() bypassed
[RootDetection Bypass] root check for package: com.ramdroid.appquarantinepro
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] return value for binary: su
[RootDetection Bypass] return value for binary: su
```

```
========
REQUEST
========
GET https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html HTTP/2.0
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (Linux; Android 10; Galaxy S10 Build/QQ1D.200105.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.186 Mobile Safari/537.36 (Mobile; afma-sdk-a-v224400999.222508000.1)
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
accept-encoding: gzip, deflate
accept-language: en-US,en;q=0.9
x-requested-with: com.timewarp.scan.bluelinefiltertiktok.free
=========
RESPONSE
=========
HTTP/2.0 200
p3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
timing-allow-origin: *
cross-origin-resource-policy: cross-origin
vary: Accept-Encoding
x-content-type-options: nosniff
content-encoding: gzip
server: cafe
content-length: 122542
x-xss-protection: 0
date: Thu, 12 Jan 2023 21:47:32 GMT
expires: Fri, 13 Jan 2023 21:47:32 GMT
cache-control: public, max-age=86400
etag: 3042398817269881164
content-type: text/html; charset=UTF-8
age: 14647
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"
```

```
Currently running services:
  DockObserver
  SurfaceFlinger
  SystemPatcher
  accessibility
  account
  activity
  activity_task
  adb
  alarm
  android.security.keystore
  android.service.gatekeeper.IGateKeeperService
  apexservice
  app_binding
  appops
  appwidget
  ashmem_device_service
  audio
  autofill
  backup
  battery
  batteryproperties
  batterystats
```