Android

Carpetas Android

```
acct: Contiene información de contabilidad de recursos, que puede ser utilizada para el seguimiento de recursos por parte del sistema.

bin: Aquí se encuentran archivos binarios ejecutables del sistema. Contiene programas y utilidades fundamentales.

boot: Contiene archivos relacionados con el proceso de arranque del sistema.

cache: Almacena datos temporales utilizados por varias aplicaciones y por el sistema operativo.

charger: Contiene archivos relacionados con la interfaz de carga del dispositivo.

data: Esta carpeta almacena datos de usuario y configuraciones de aplicaciones. Los datos de usuario y algunas configuraciones específicas de la aplicación se encuentran aquí.

dev: Contiene nodos de dispositivos que representan dispositivos de hardware y otros recursos del sistema.

etc: Contiene archivos de configuración del sistema y de aplicaciones. Configuraciones del sistema, archivos de hosts, y otros archivos de configuración pueden estar presentes aquí.

lib: Contiene bibliotecas compartidas utilizadas por aplicaciones y el sistema.

mnt: Se utiliza como un punto de montaje temporal para dispositivos externos o sistemas de archivos adicionales.
```

oem: Contiene archivos y configuraciones específicas del fabricante del dispositivo.

proc: Proporciona información en tiempo real sobre el estado del sistema y los procesos en ejecución.

sbin: Similar a la carpeta "bin", pero contiene archivos binarios ejecutables que requieren privilegios de superusuario para ejecutarse.

sys: Contiene información y configuraciones del kernel del sistema operativo.

system: Almacena el sistema operativo Android propiamente dicho, incluyendo las aplicaciones del sistema.

vendor: Contiene archivos específicos del fabricante o proveedor del hardware.

vendor_file_contexts: Archivos de contexto que especifican las reglas de acceso para archivos en el directorio "vendor".

vendor_seapp_contexts: Archivos de contexto de seguridad para aplicaciones del sistema del proveedor.

vendor_service_contexts: Archivos de contexto de seguridad para servicios del sistema del proveedor.

etc/fstab.android_x86_64: Archivo que describe cómo se deben montar los diferentes sistemas de archivos durante el proceso de arranque.

init: Contiene archivos de inicialización y configuración del sistema.

lib: Bibliotecas compartidas utilizadas por aplicaciones y

```
el sistema.
sepolicy: Políticas de seguridad que controlan los permisos
y accesos del sistema.
```

Conectar a Android

```
adb connect IP
```

transferir archivo a android

```
sudo adb push text.txt /sdcard/
```

transferir de android a kali

```
sudo adb pull /sdcard/text.txt
```

shell

```
adb shell
```

Instalar apk

```
sudo adb install InsecureBankv2.apk
```

Ver propiedades del android

```
pm list packages → Te dice todos los paquetes que están ins
talados en el móvil

getprop → Propiedades del Android es parecido a System info

dumpsys → Da información del sistema
```

ingenieria reversa, obtener codigo de apk

```
sudo apktool d -s dvhma.apk
```

Cambiar clase .dex a .jar

```
sudo enjarify classes.dex -o classes.jar
```

ver .jar

```
sudo jadx-gui
```

Modificar fichero de apk

```
nano /Android/InsecureBankv2/res/values/strings.xml
```

firmar apk

```
sudo java -jar /home/kali/Software/AplicacionesMóviles/Uber-APK-Signer/uber-apk-signer-1.1.0.jar -a dist -out dvhma_mod.apk
```

Mobsf (Analisis estatico)

```
sudo docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
```

Analisis Dinamico

```
sudo docker run -it --rm -p 8000:8000 -p 1337:1337 -eMOBSF_ANALYZER_IDENTIFIER=10.0.10.10:5555 opensecurity/mobile-security-framework-mobsf:latest
```