



Name : Ahmed Alzahrani || **Email :** You-187@hotmail.com

Mobile Pentesting

Connect to your device (make sure emulator is in Bridged!!)

```
santoku@santoku: ~  
File Edit Tabs Help  
santoku@santoku:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:33:3d  
          inet addr:192.168.100.9  Bcast:192.168.100.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fef6:333d/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:224 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:181 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:21388 (21.3 KB)  TX bytes:16233 (16.2 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:280 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:280 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:23034 (23.0 KB)  TX bytes:23034 (23.0 KB)  
  
santoku@santoku:~$ adb connect 192.168.100.10  
* daemon not running. starting it now on port 5037 *  
* daemon started successfully *  
connected to 192.168.100.10:5555  
santoku@santoku:~$
```

Find an interesting apk, or multiple apk's and download them to Santoku

```
santoku@santoku: ~  
File Edit Tabs Help  
root@vbox86p:/storage/emulated/legacy/download # ls  
Instagram_v212.0.0.38.119_apkpure.com.apk  
open_gapps-x86-4.4-pico-20210126.zip  
open_gapps_debug_logs.tar.gz  
open_gapps_log.txt  
root@vbox86p:/storage/emulated/legacy/download # pwd  
/storage/emulated/legacy/download  
root@vbox86p:/storage/emulated/legacy/download # exit  
santoku@santoku:~$ adb pull /storage/emulated/legacy/download Instagram_v212.0.0.  
.38.119_apkpure.com.apk  
pull: building file list...  
pull: /storage/emulated/legacy/download/Instagram_v212.0.0.38.119_apkpure.com.ap  
k -> Instagram_v212.0.0.38.119_apkpure.com.apk/Instagram_v212.0.0.38.119_apkpure  
.com.apk  
pull: /storage/emulated/legacy/download/open_gapps_debug_logs.tar.gz -> Instagram_v212.0.0.  
.38.119_apkpure.com.apk/open_gapps_debug_logs.tar.gz  
pull: /storage/emulated/legacy/download/open_gapps_log.txt -> Instagram_v212.0.0.38.119_ap  
kpure.com.apk/open_gapps_log.txt  
pull: /storage/emulated/legacy/download/open_gapps-x86-4.4-pico-20210126.zip -> Instagram_  
v212.0.0.38.119_apkpure.com.apk/open_gapps-x86-4.4-pico-20210126.zip  
4 files pulled. 0 files skipped.  
3446 KB/s (108810652 bytes in 30.831s)  
santoku@santoku:~$ ls  
Desktop Downloads Music Public Videos  
Documents Instagram_v212.0.0.38.119_apkpure.com.apk Pictures Templates  
santoku@santoku:~$
```

Install that app remotely

```
santoku@santoku: ~/Ludo
File Edit Tabs Help
santoku@santoku:~$ adb install Ludo King™_v6.5.0.202_apkpure.com.apk
can't install 'Ludo' because it's not a file
santoku@santoku:~$ cd ludo
bash: cd: ludo: No such file or directory
santoku@santoku:~$ ls
Desktop  Instagram_v212.0.0.38.119_apkpure.com.apk  Music  Templates
Documents  Ludo  Pictures  Videos
Downloads  Ludo King™_v6.5.0.202_apkpure.com.apk  Public
santoku@santoku:~$ cd Ludo
santoku@santoku:~/Ludo$ ls
Instagram_v212.0.0.38.119_apkpure.com.apk  open_gapps_log.txt
open_gapps_debug_logs.tar.gz  open_gapps-x86-4.4-pico-20210126.zip
santoku@santoku:~/Ludo$ adb install Ludo King™_v6.5.0.202_apkpure.com.apk
can't find 'Ludo' to install
santoku@santoku:~/Ludo$ ls
Instagram_v212.0.0.38.119_apkpure.com.apk  open_gapps_log.txt
Ludo King™_v6.5.0.202_apkpure.com.apk  open_gapps-x86-4.4-pico-20210126.zip
open_gapps_debug_logs.tar.gz
santoku@santoku:~/Ludo$ adb install Ludo King™_v6.5.0.202_apkpure.com.apk
can't find 'Ludo' to install
santoku@santoku:~/Ludo$ ls
Instagram_v212.0.0.38.119_apkpure.com.apk  open_gapps_log.txt
LudoKing™_v6.5.0.202_apkpure.com.apk  open_gapps-x86-4.4-pico-20210126.zip
open_gapps_debug_logs.tar.gz
santoku@santoku:~/Ludo$ adb install LudoKing™_v6.5.0.202_apkpure.com.apk
248 KB/s (58290675 bytes in 228.774s)
Error: Could not access the Package Manager. Is the system running?
santoku@santoku:~/Ludo$ adb devices
List of devices attached
192.168.100.11:5555    device
```