Mobile Penetration Testing - Final Project

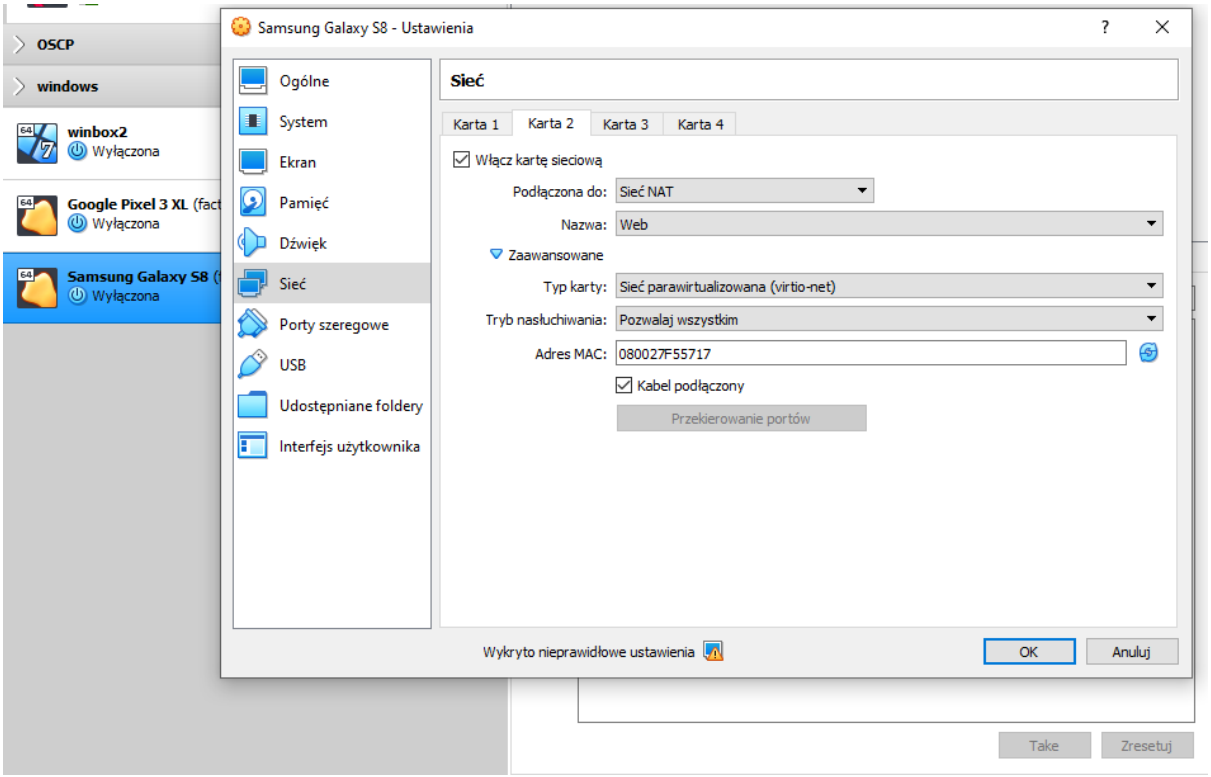
Paweł Kamiński

Global Red Extended Course

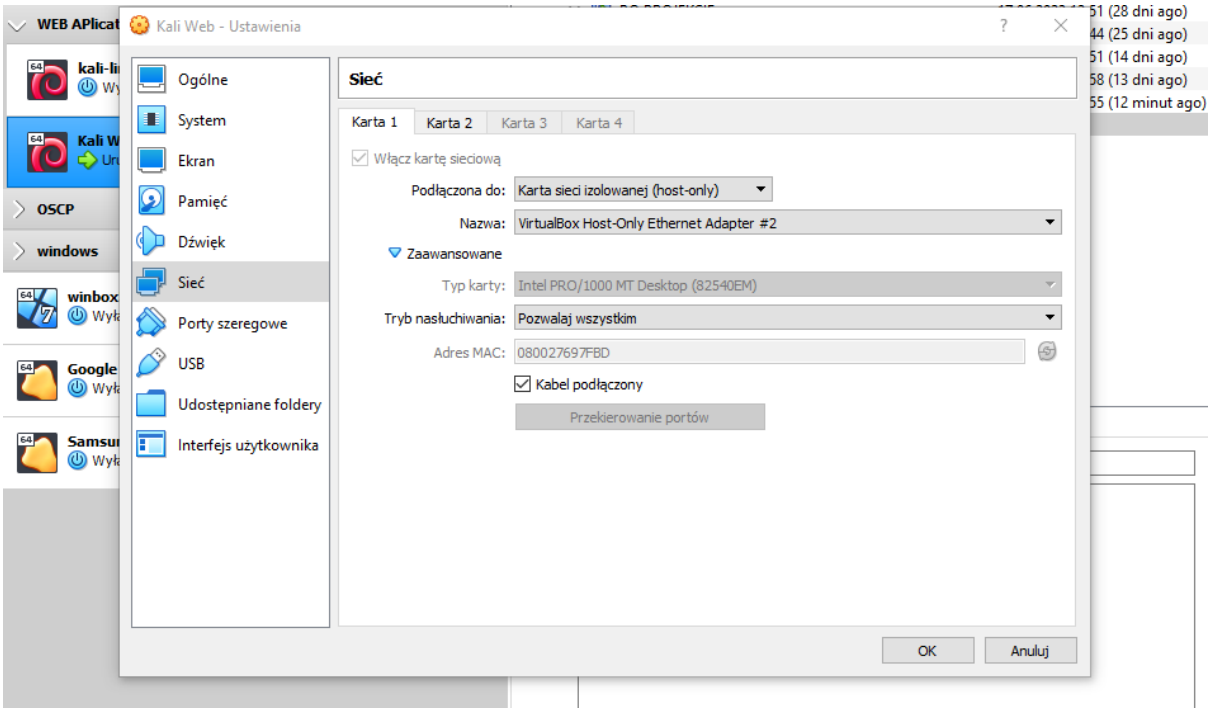
RM270822UW1

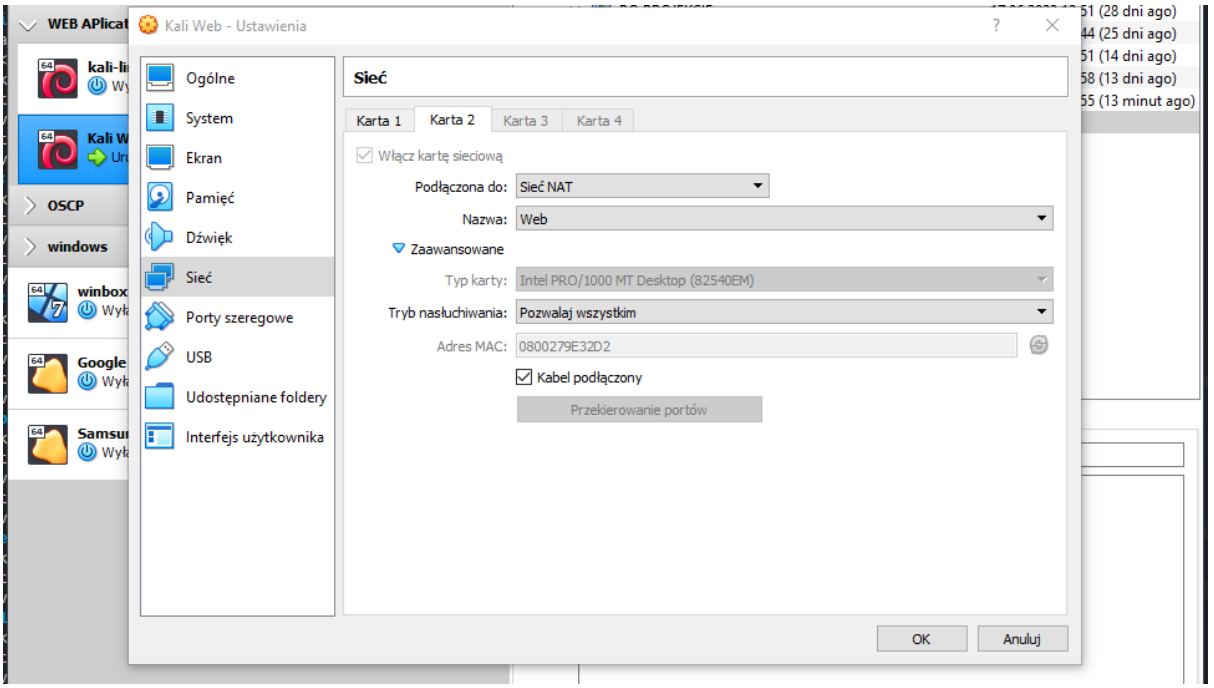
Part 1

1) Creating a new Nat network called “Web”



2) IP Configuration





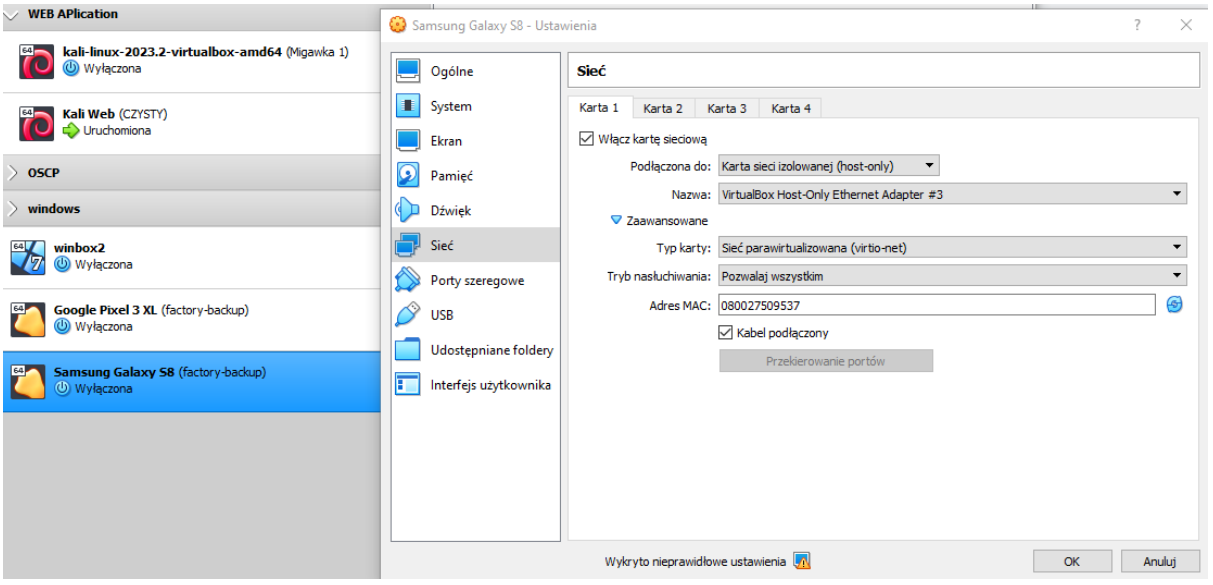
3) Setting static IP on kali “/etc/network/interfaces”
Mine Nat network is on 2nd card that’s why I have to set eth1, because eth0 is my “host-only” card.

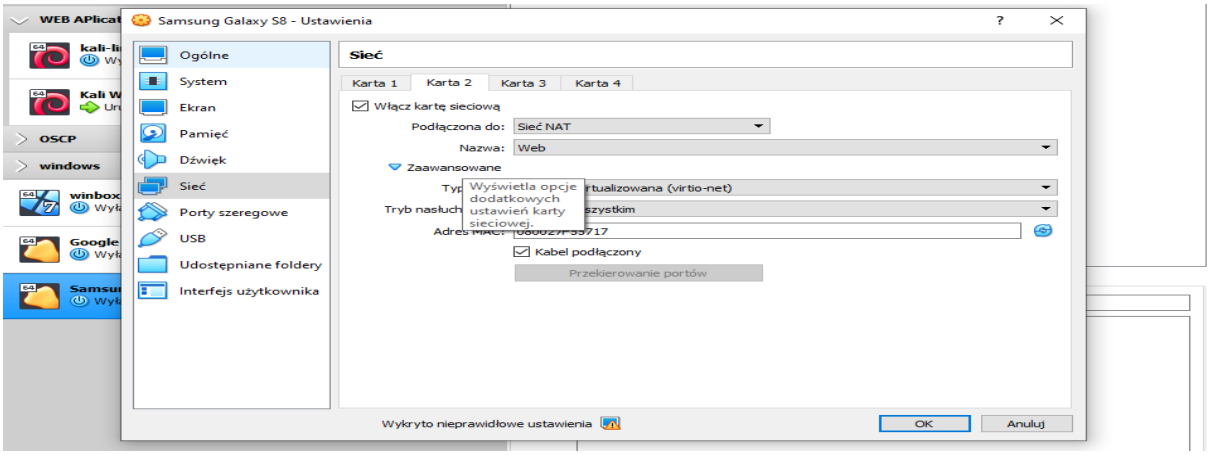
```
kali@kali: /
File  Actions  Edit  View  Help
  GNU nano 7.2                                                    /et
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
#auto lo
#iface lo inet loopback

auto eth1
iface eth1 inet static
address 10.0.2.4/24
gateway 10.0.2.1
```

```
┌──(kali㉿kali)-[/etc/network/interfaces.d]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:69:7f:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.84.105/24 brd 192.168.84.255 scope global dynamic noprefixroute eth0
       valid_lft 505sec preferred_lft 505sec
    inet6 fe80::772f:d642:4dc6:6bac/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9e:32:d2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9e:32d2/64 scope link
       valid_lft forever preferred_lft forever
```

Part 2

Network setting on my mobile phone:





Part 3

1) Installing Docker, Apache and Sql are pre installed by default, we just have to start them:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update --fix-missing
[sudo] password for kali:
Get:1 http://kali.koyanet.lv/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.koyanet.lv/kali kali-rolling/main amd64 Packages [19.3 MB]
Get:3 http://kali.koyanet.lv/kali kali-rolling/main amd64 Contents (deb) [45.
5 MB]
Get:4 http://kali.koyanet.lv/kali kali-rolling/contrib amd64 Packages [115 kB
]
Get:5 http://kali.koyanet.lv/kali kali-rolling/contrib amd64 Contents (deb) [
219 kB]
Get:6 http://kali.koyanet.lv/kali kali-rolling/non-free amd64 Packages [218 k
B]
Get:7 http://kali.koyanet.lv/kali kali-rolling/non-free amd64 Contents (deb)
[918 kB]
Fetched 66.4 MB in 10s (6,881 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
583 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install docker -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
```

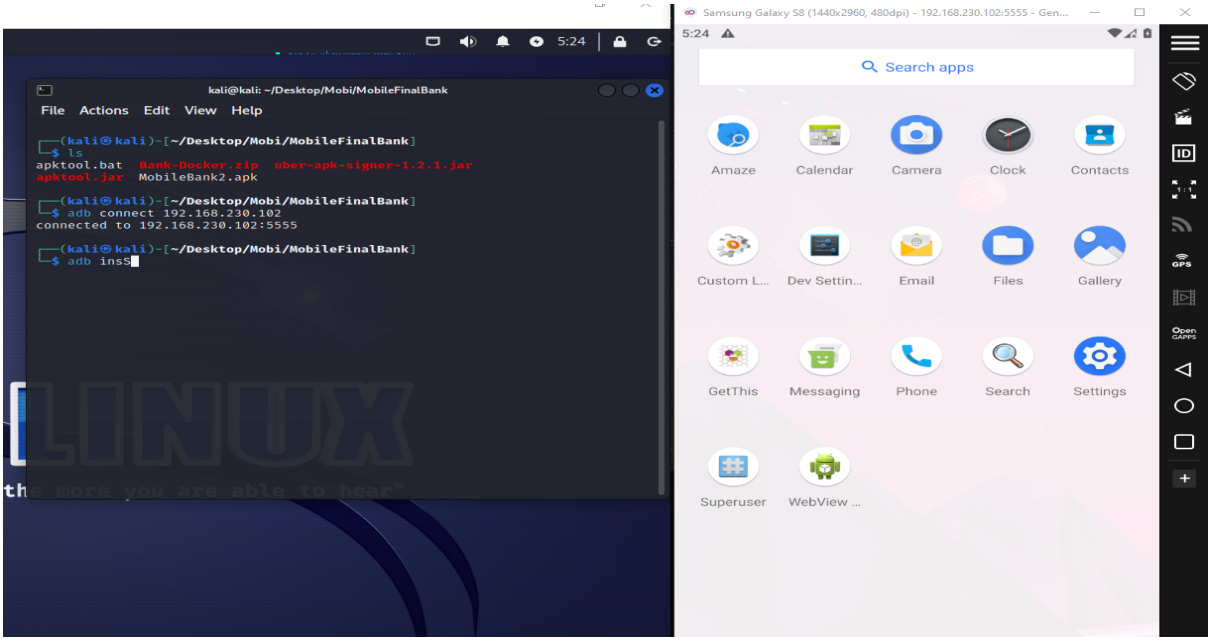
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install docker-compose -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  cgroupfs-mount containerd criu docker.io libintl-perl libintl-xs-perl
  libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl
  libsort-naturally-perl needrestart python3-docker python3-dockerpty runc
  tini
Suggested packages:
  containernetworking-plugins docker-doc aufs-tools btrfs-progs debootstrap
  rinse rootlesskit xfsprogs zfs-fuse | zfsutils-linux
The following NEW packages will be installed:
  cgroupfs-mount containerd criu docker-compose docker.io libintl-perl
  libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl
  libproc-processtable-perl libsort-naturally-perl needrestart
  python3-docker python3-dockerpty runc tini
0 upgraded, 16 newly installed, 0 to remove and 583 not upgraded.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install adb -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  android-libbase android-libboringssl android-libcutils android-liblog
  android-sdk-platform-tools-common
The following NEW packages will be installed:
  adb android-libbase android-libboringssl android-libcutils android-liblog
  android-sdk-platform-tools-common
0 upgraded, 6 newly installed, 0 to remove and 583 not upgraded.
Need to get 998 kB of archives.
After this operation, 3,189 kB of additional disk space will be used.
Get:1 http://kali.koyanet.lv/kali kali-rolling/main amd64 android-liblog amd6
4 1:29.0.6-28 [40.3 kB]
```

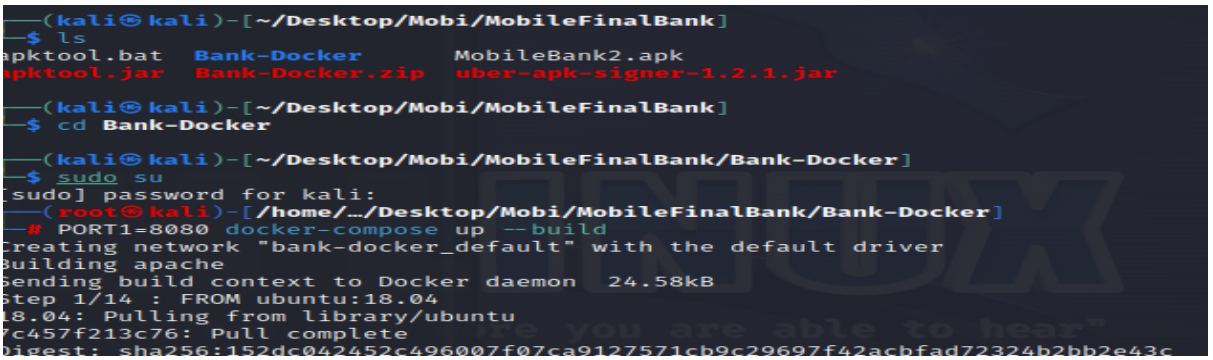
Starting apache and Sql:

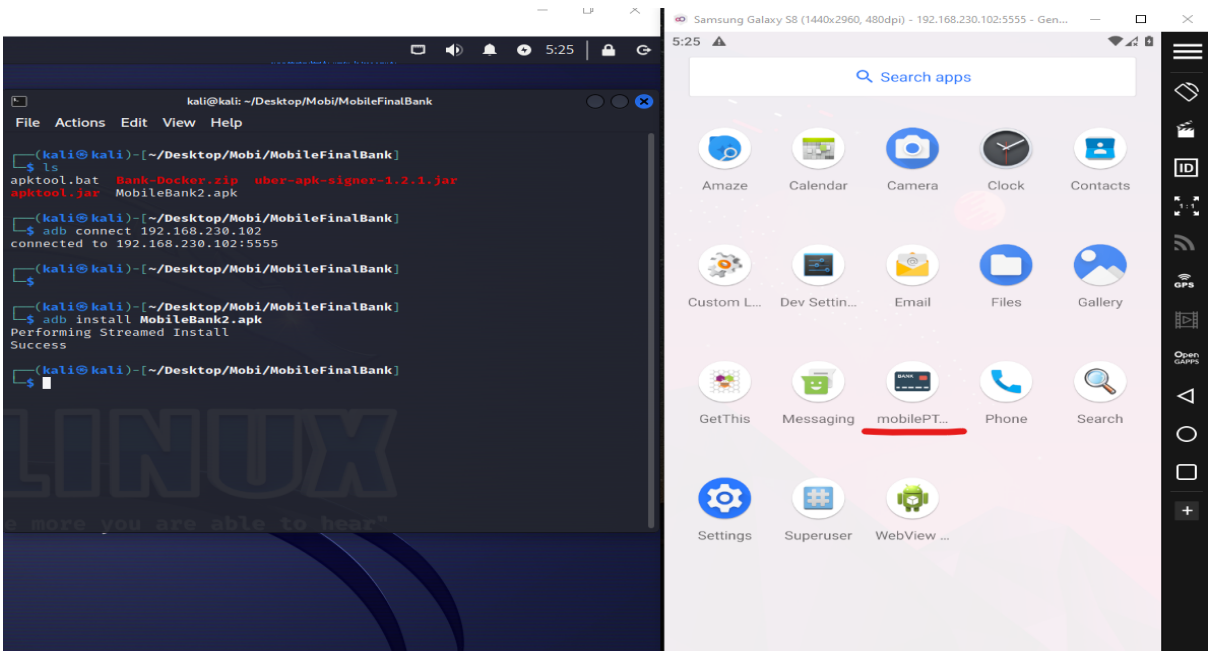
```
┌──(kali㉿kali)-[~]
└─$ sudo service postgresql start

┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start

┌──(kali㉿kali)-[~]
└─$ sudo service --status-all |grep -i sql
 [ + ]  postgresql
^[[A^[[A^[[A

┌──(kali㉿kali)-[~]
└─$ sudo service --status-all |grep -i apache
 [ - ]  apache-htcacheclean
 [ + ]  apache2
```

2) installing APK and building docker

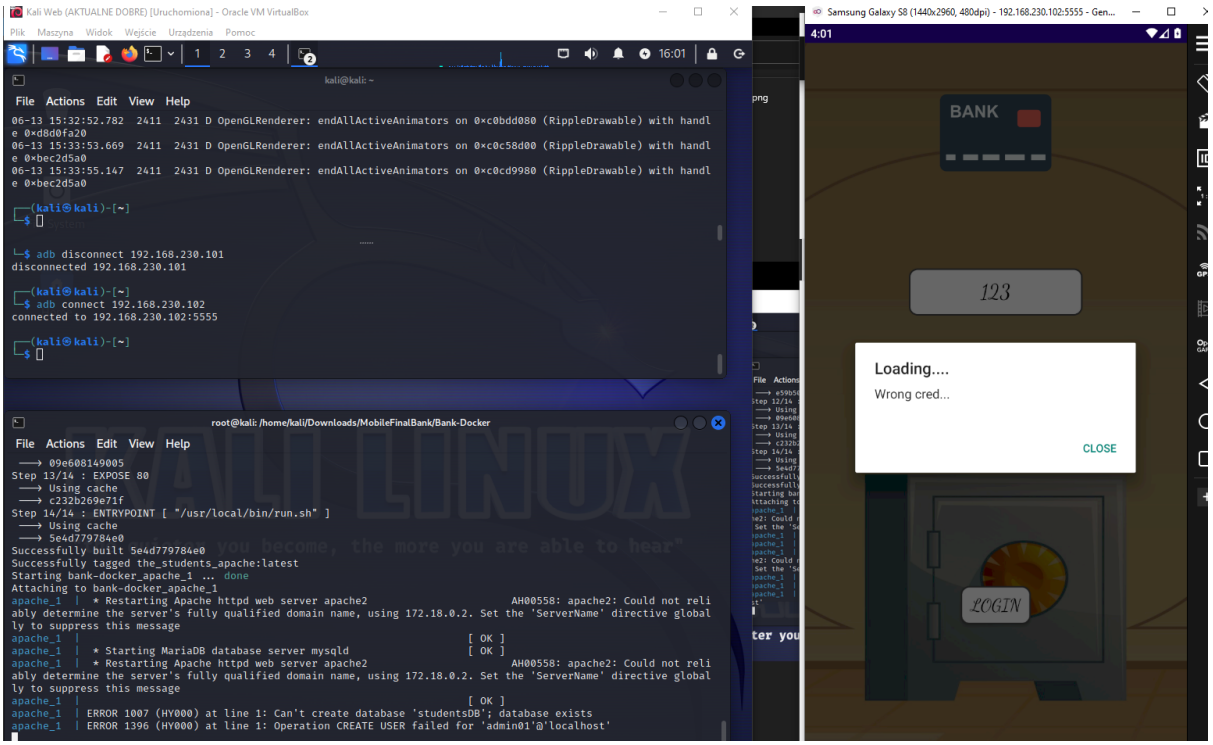


Building Docker:



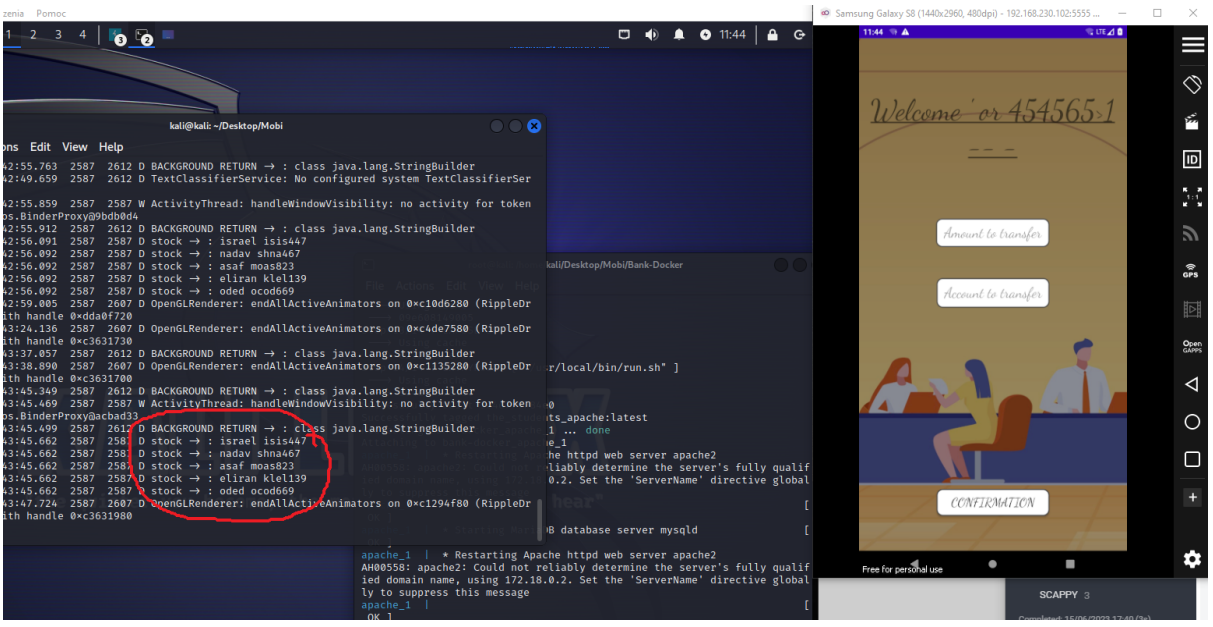


At first, I'm checking that application is connected to database:
But I would like to add that I had some troubles connecting with device 192.168.230.101 so I had to add another one to Genymotion and everything worked fine.

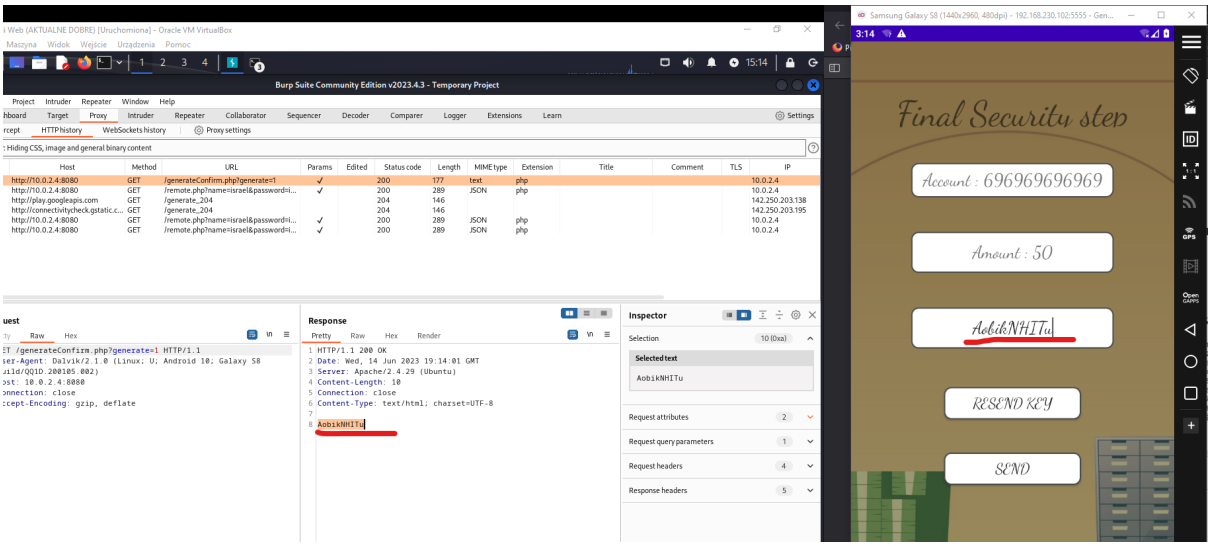


“Wrong cred…” This means we’re connected to a database, otherwise we would see “No connection to database…”

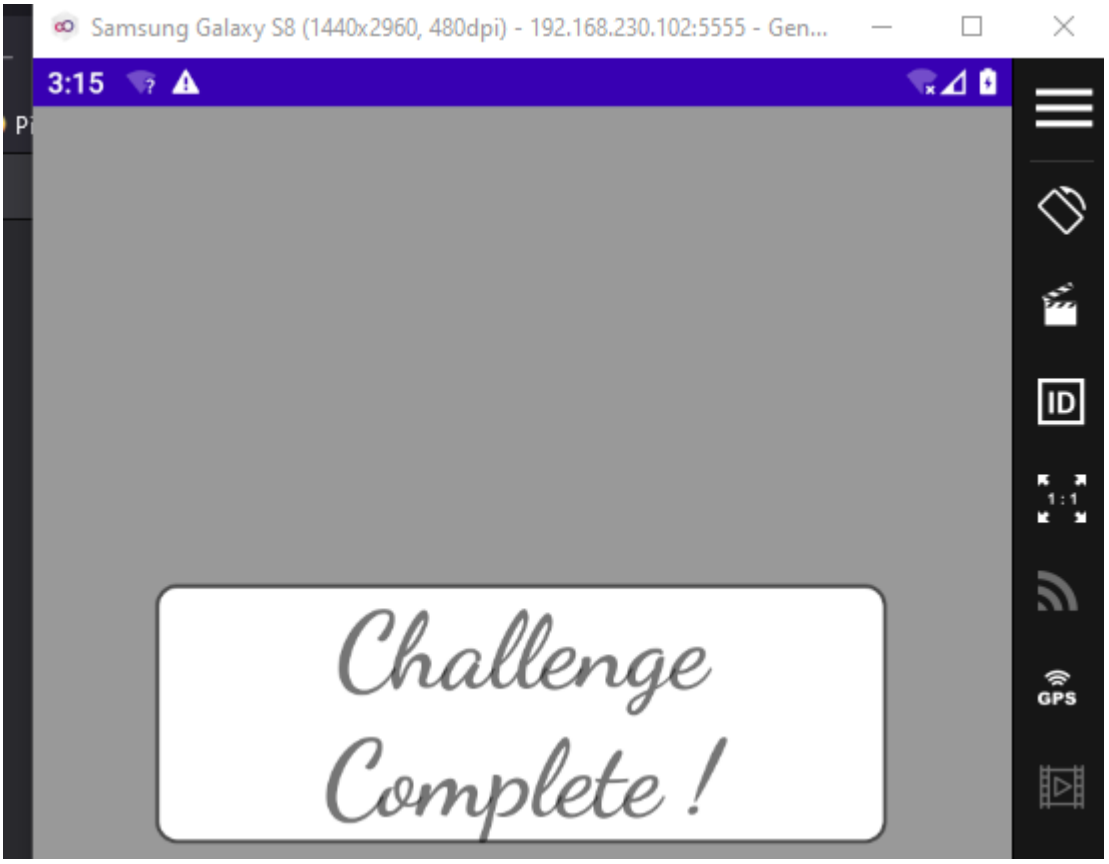
Now I have to perform Boolean SQLi and use logcat to catch credentials:



Sweet, now let's login using one of them but unfortunately the maximum amount to transfer is 50, so let’s try to send 50 ;)
For this I’ll have to set up Burp too ;)



I’ve got the message.



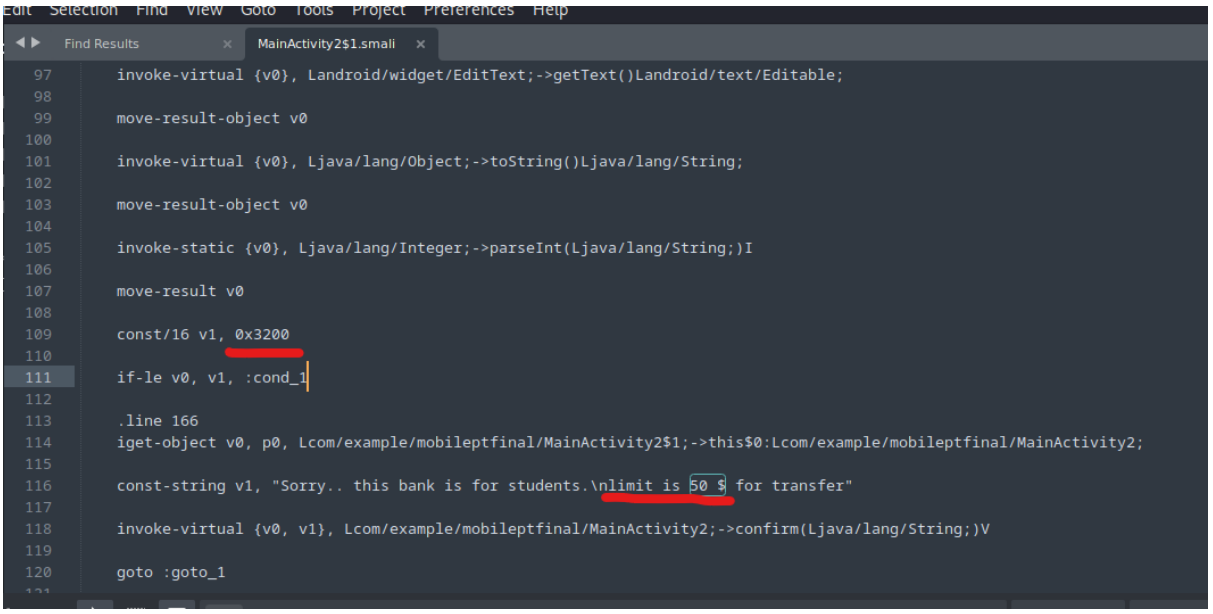
Nicely done…

Now to have the possibility of transferring 4000$ I have to decompile the app and find part of the code responsible for these restrictions.

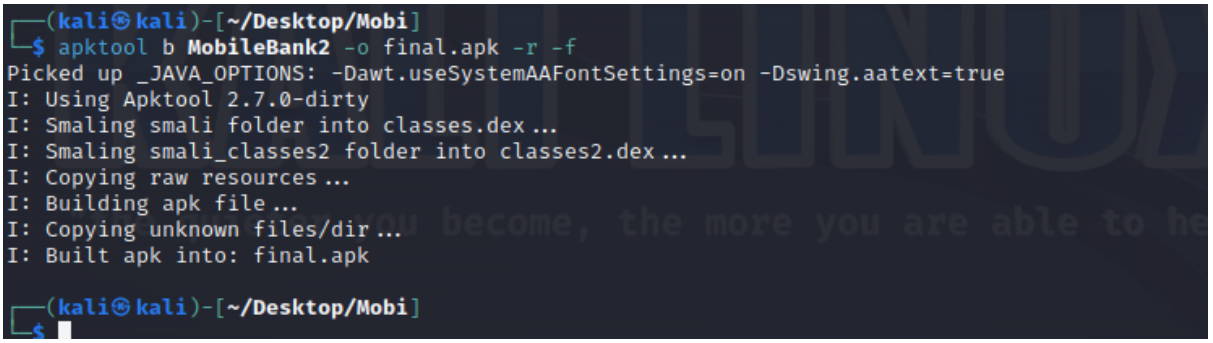
Decompilation:

```
┌──(kali㉿kali)-[~/Desktop/Mobi]
└─$ apktool d MobileBank2.apk -r -f
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on MobileBank2.apk
I: Copying raw resources ...
I: Baksmaling classes.dex ...
I: Baksmaling classes2.dex ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...
```

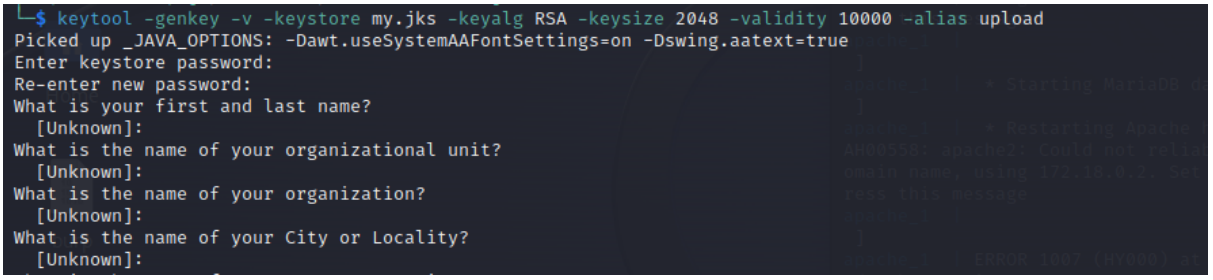
Part of the code responsible for the max amount to transfer “0x32” which is 50 in hexadecimal, let’s put a couple 0’s more there 👍



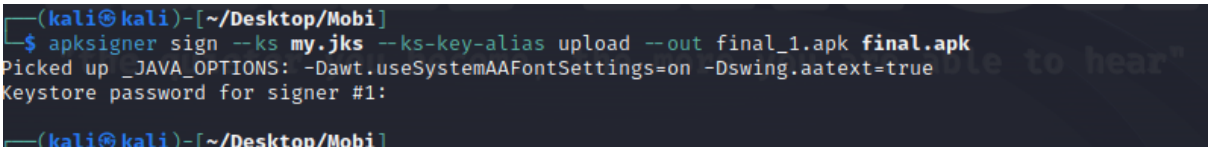
Now building new app (after changes)



Generating Certificate to sing this app

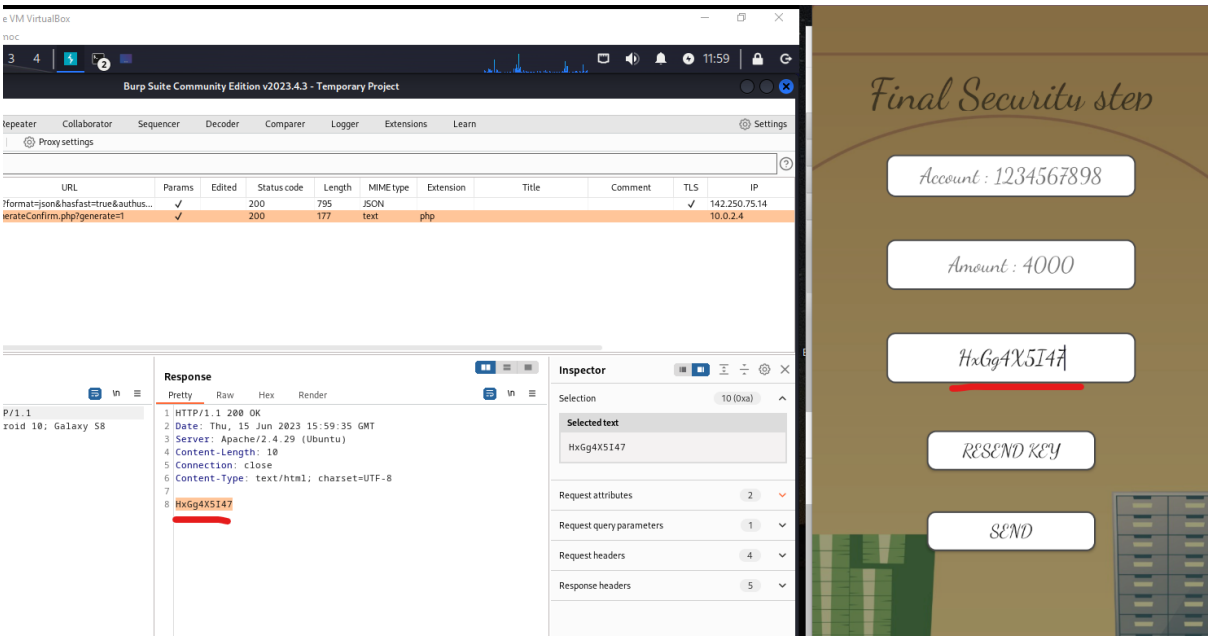


Signing



Now I’m searching this app on the phone using adb, uninstalling it and installing the new (changed) one.

Now Lets see if it’s working:



Catching key by Burp and ….

Taa daaam 🙂

Thank You for this challenge I learned a lot, mostly because I’ve got lots of trouble during configurations but thanks to that I gained knowledge and experience.
Liked it a lot ! :)