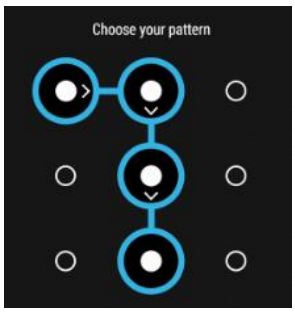
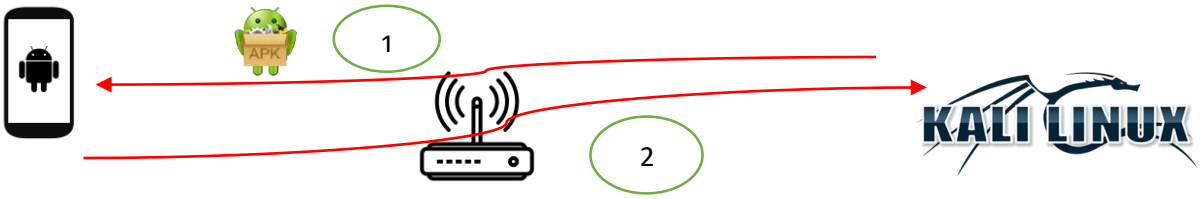
Excersie – Breaking Login Pattern





This exercise address the possibility of having a physical access to a root device, where this android device may belong to your friend or wife/husband. Using some social engineering skills you could have the device in hand for few minutes, before doing anything you should prepare your APK to automate the grabbing of a KEY file named "gesture.key" which is located at "/data/system/gesture.key" decoding this key file will allow us to know the target login pattern and eventually unlock his device whenever you want.

Step 1

Prepare and test your APK properly, then upload your APK on a webserver like apache on your Kali device. Make sure that to have IP connectivity between the Kali and the target's phone.

Step 2

Once you have a physical access to your target, open up a browser, download and install your malicious APK, make sure to remove it once the file gets transferred (the file size is usually less than 2 KB so it shouldn't take that long)

Step 3

Use Andriller to decode the "gesture.key"