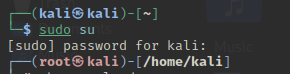
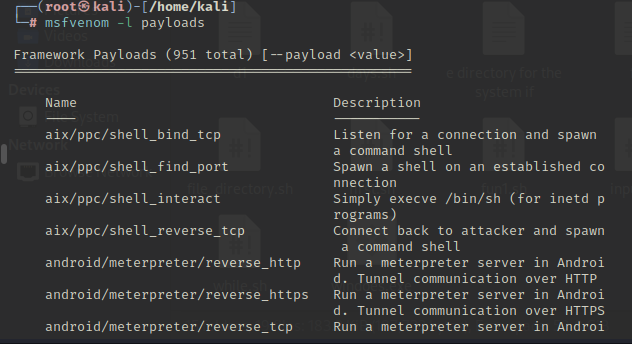
There are total two steps for doing the work . First is to make a payload for the target machine and then making exploit for conduct the exploitation .

First step (make payload ):

* Give the terminal permission to root :

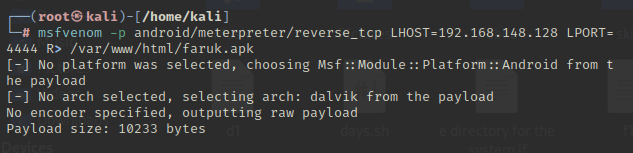


* Then show all the metasploit payloads using command :



It will show all the list of payloads .

* Among them select the suitable payloads related to android reverse tcp .



Set LHOST = (Attacker IP address - 192.168.148.128

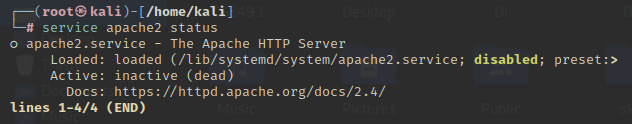
Set LPORT = Listening port . It could be any active port . I have taken 4444

I’m putting my apk file in the apache server . So I have given the server path of apk file path is (/var/www/html/)

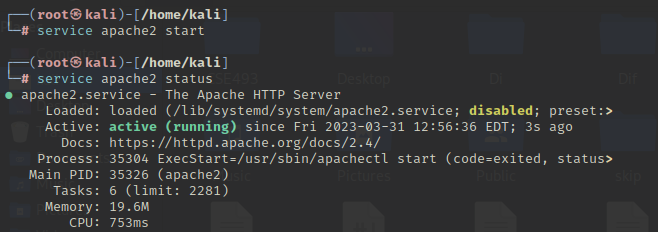
And I put the application name is faruk and the file extension is apk .

After pressing enter it will take some time and create a apk file to the web apache server .

* I need to activate the apache server . So I need to check the server status first . for checking the server status :



As it is showing the server status is inactive so I need to activate the server . By doing this anyone can access the apk file remotely . For activing the server I need to do :

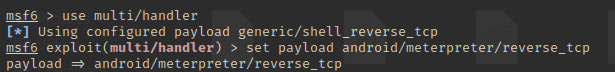


Second Step (Exploiting )

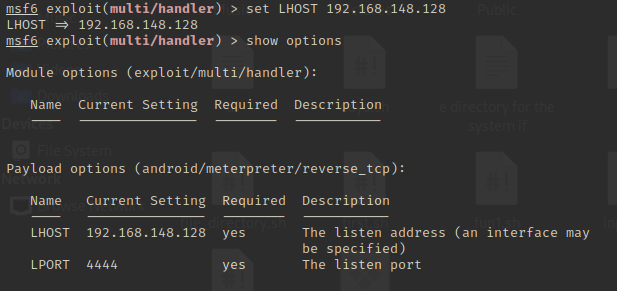
* First I need to enter into the console .



* Then I need to enter into he multi handler and select the payload .



* Then I need to check the options of the payloads and need to select the LHOST and LPORT for the attacker machine .



* After all these I need to type ‘exploit’ and then the session will generate and waiting for the exploitation . When someone will download or receive the apk file and install it session will start and attacker will get the full access of the target android machine .

