

Android Mobile Pentest 101

© tsug0d, September 2018

Lecture 10.3 – Creating Exploit: Android Activity

Mục tiêu: Hiểu Android Activity là gì

Introduction

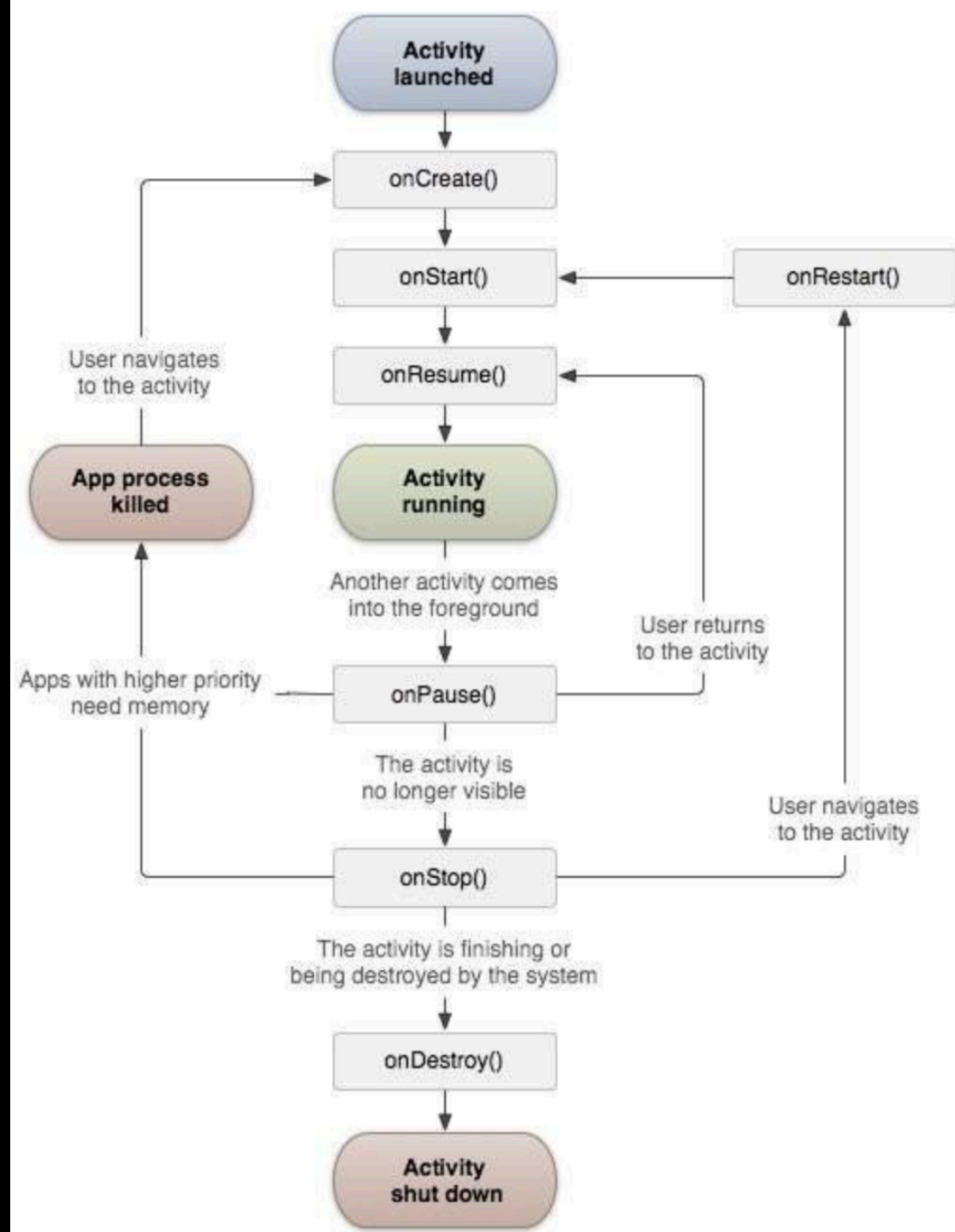
- Bài này giúp bạn hiểu được thế nào là 1 Activity trong android

What's Activity?

- Được đề cập ở đây: <https://developer.android.com/reference/android/app/Activity>
- Activity đại khái là 1 hành động mà user có thể thực hiện.
- Nếu bạn từng code C, C++ hay bất kì ngôn ngữ nào thì activity gần như là 1 cái hàm code ra để chờ được gọi lên (gần như chứ không giống hoàn toàn, trong activity còn có callback)

What's Activity?

- Bên trong 1 activity: có nhiều callback như onCreate(), onStart(), blah blah



What's Activity?

<code>onCreate()</code>	Được gọi khi activity được khởi tạo
<code>onStart()</code>	Được gọi khi activity bắt đầu hiện lên cho user thấy
<code>onResume()</code>	Được gọi khi activity được user sử dụng
<code>onPause()</code>	Được gọi khi user “focus” qua 1 activity khác
<code>onStop()</code>	Được gọi khi activity không còn được nhìn thấy bởi user
<code>onDestroy()</code>	Được gọi trước khi activity bị hệ thống xóa
<code>onRestart()</code>	Được gọi khi activity được bật lên lại sau khi Stop

Let's dev

- Bây giờ chúng ta sẽ code 1 tí để hiểu thêm nha
- Tạo hết callback trong **MainActivity.java**, sau đó code Log.i để xem khi nào callback trong activity được gọi lên

Ví dụ:

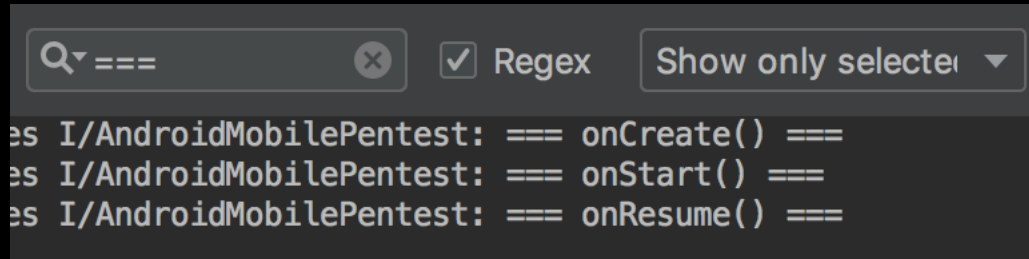
```
@Override
protected void onStart()
{
    super.onStart();
    Log.i(msg, "=== onStart() ===");
}
```

- Code mẫu:

https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java_activities

Let's dev

- Chạy thử cái code nào, trong logcat hiện cái này:

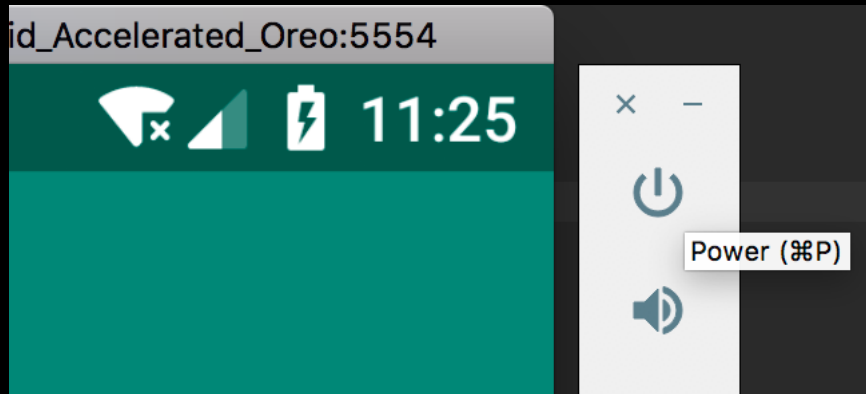


```
es I/AndroidMobilePentest: === onCreate() ===  
es I/AndroidMobilePentest: === onStart() ===  
es I/AndroidMobilePentest: === onResume() ===
```

- Chúng ta vừa chạy code nên activity sẽ được gọi lên, onCreate() is triggered
- Activity đang hiện lên dần dần, onStart() triggered
- Hiện ra hoàn toàn, onResume() triggered

Let's dev

- Bây giờ click thử vào nút shutdown để lock cái phone lại:



- Logcat:

```
I/AndroidMobilePentest: === onCreate() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===
```

- Vì chúng ta vừa gọi cái activity Lock Phone (là 1 activity khác), activity của chúng ta không còn được “focus” nữa, nên onPause() triggered
- Sau khi lock rồi, không còn hiện nữa, nên onStop() triggered.

Let's dev

- Bấm nút power vừa nảy để mở phone lên laiuj:

```
I/AndroidMobilePentest: === onCreate() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===
```

- onStart() & onResume() hiện trong logcat, tự hiểu nha 😊
- Tắt app:

```
I/AndroidMobilePentest: === onCreate() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===  
I/AndroidMobilePentest: === onDestroy() ===
```