

## Android RE (25 Point)

Tải file app.apk

android  
25

app.apk

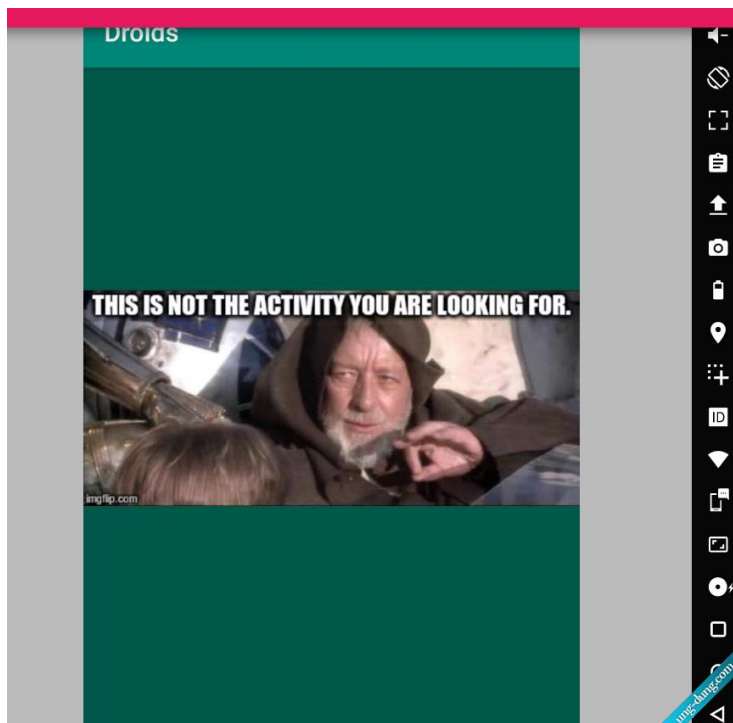
Flag

Submit

ung-dung.com

Cài phần mềm giả lập android ví dụ: LDPlayer

Cài đặt app.apk đó lên trình giả lập đó



Ta thấy đây là một hình ảnh với nội dung thông báo là "**This is not the active....**" --> Bí ẩn nằm trong tám ảnh này chúng ta cần giải mã Cài đặt công cụ apktool trên

kali <https://ibotpeaches.github.io/Apktool/install/> Chạy công cụ apktool để giải mã file app.apk

```
root@ThangMT:~/Desktop# apktool d app.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1 on app.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values ** XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
root@ThangMT:~/Desktop#
```

Vào thư mục app vừa giải mã, chúng ta sẽ quan tâm đến thư mục **smali** nơi chứa thông tin về đoạn code chương trình để gọi đến file tài nguyên(theo ý hiểu của mình).

```
root@ThangMT:~/Desktop# cd app/
root@ThangMT:~/Desktop/app# ls
AndroidManifest.xml  apktool.yml  original  res  smali
```

Tiếp theo đó vào thư mục **com/example/blink/** nơi có chứa thông tin mà chúng ta cần tìm. Bạn chạy lệnh tìm kiếm :

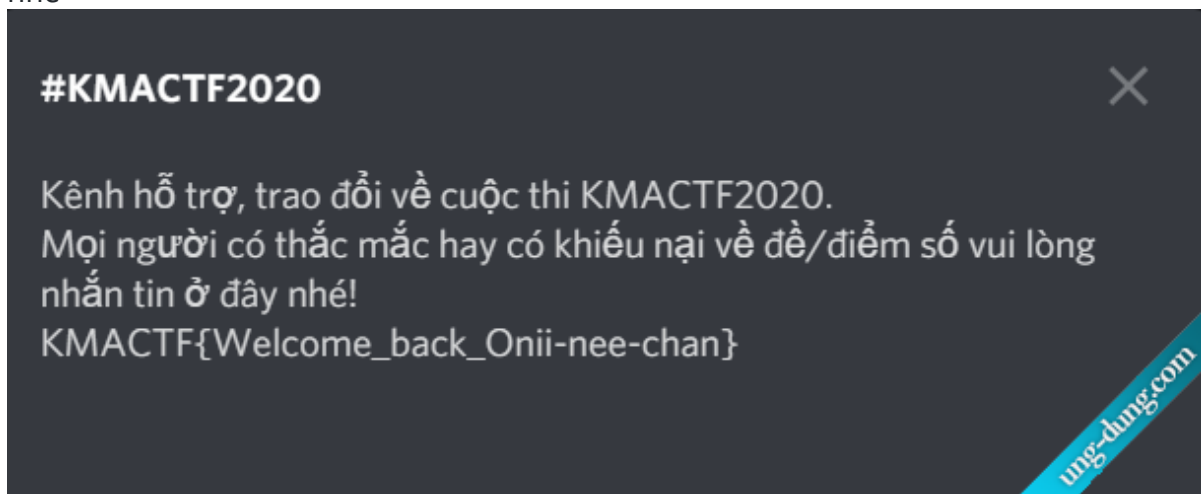
```
``` cat * | grep -i "ctf" ```
```

copy đoạn code đó và sử dụng trình base64 decode Kết quả:

**\*\*KMACTF{blink\_blink}\*\***

## Hello\_KMA ( 5 point)

Đăng ký tài khoản trên trang discord: <https://discord.gg/2QeBsgt> Nó ở ngay trên đầu nhé



## Miku (20 point)

Kiểm tra mã nguồn trang vào mục Application (f12)

