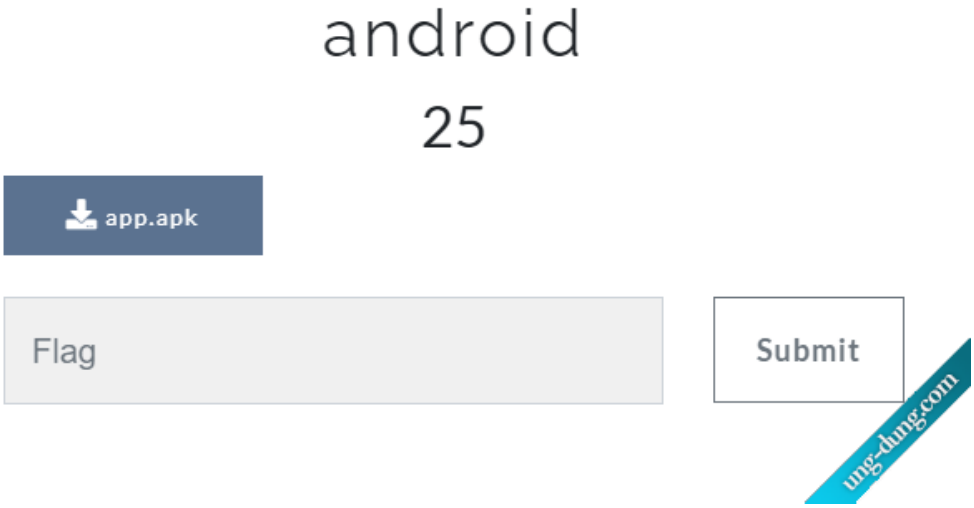
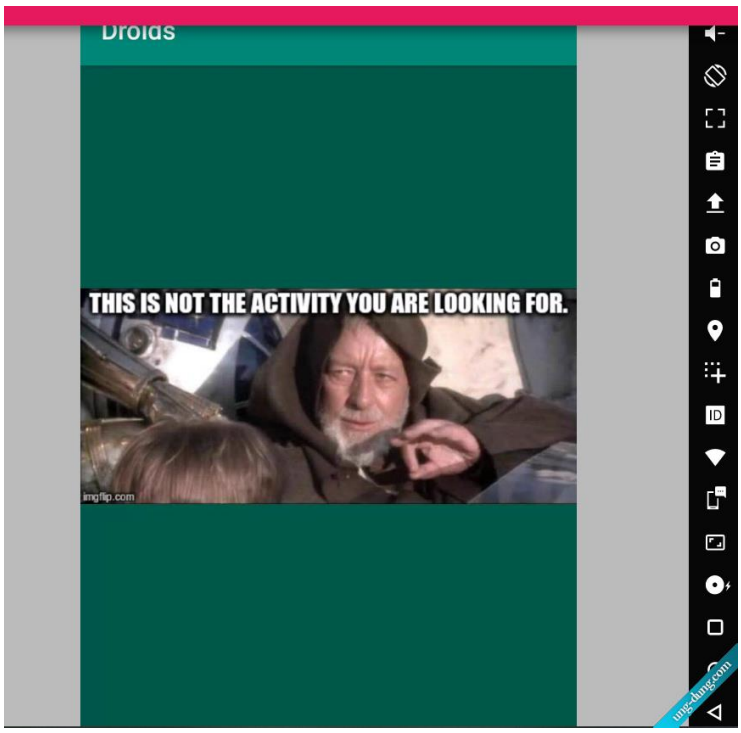
Android RE (25 Point)

Tải file app.apk



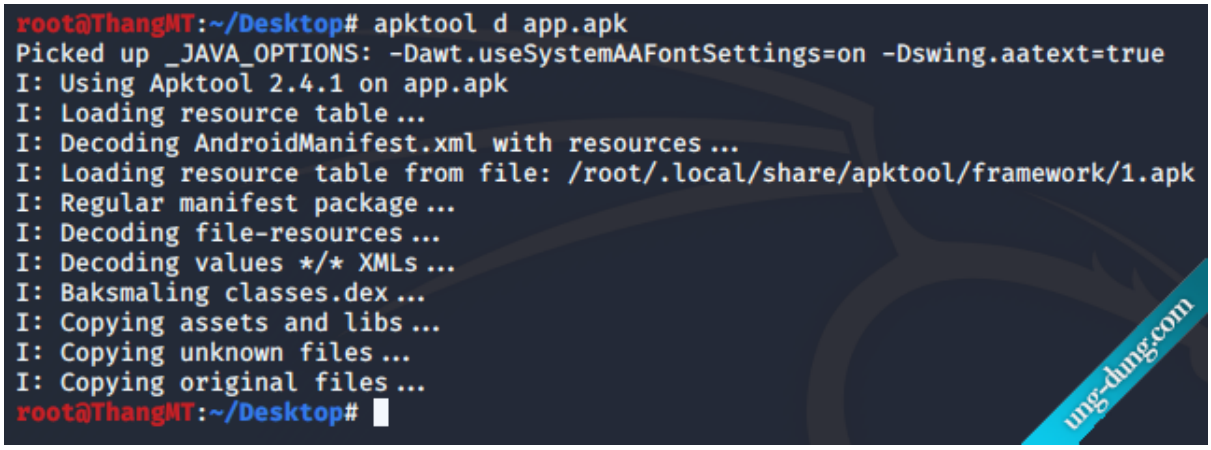
Cài phần mềm giả lập android ví dụ: LDPlayer

Cài đặt app.apk đó lên trình giả lập đó

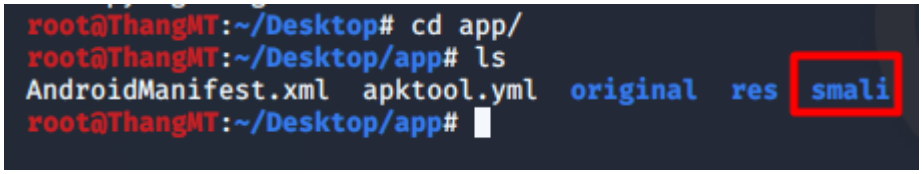


Ta thấy đây là một hình ảnh với nội dung thông báo là "**This is not the active....**" --> Bí ẩn nằm trong tấm ảnh này chúng ta cần giải mã Cài đặt công cụ apktool trên

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



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).



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

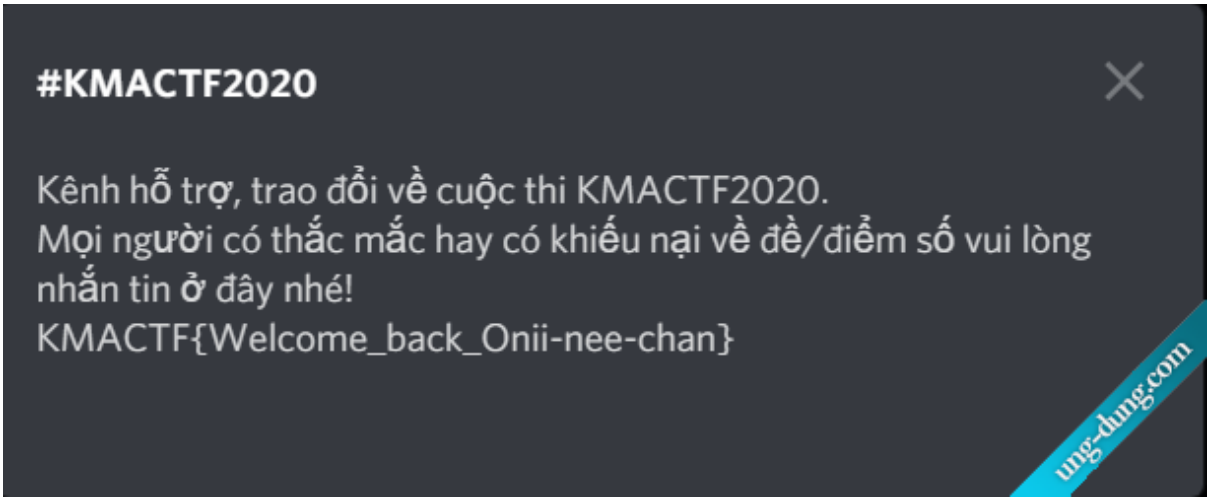
``` cat * | grep -i "ctf" ```


```

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 decord: https://discord.gg/2QeBsgt Nó ở ngay trên đầu
nhé



Miku (20 point)

Kiểm tra mã nguồn trang vào mục Application (f12)