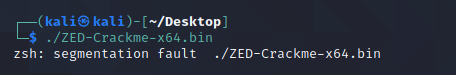
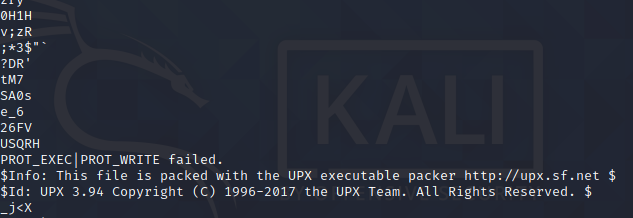
*Nguyễn Mỹ Quỳnh 19520241*

**ZED-Crackme**

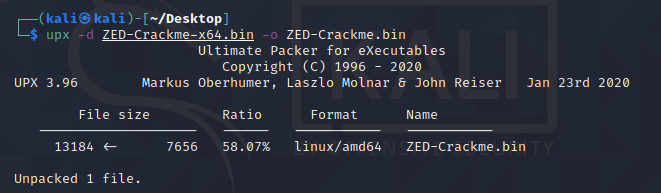
Chạy thử chương trình



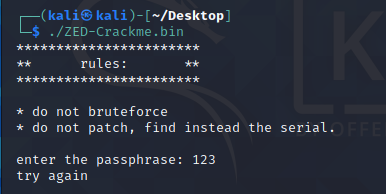
Có thể chương trình đã bị pack, dùng strings ta thấy đúng như dự đoán.



Tiến hành dùng lệnh để unpack “upx -d ZED-Crackme-x64.bin -o ZED-Crackme.bin”



Chạy thử chương trình sau khi unpack



Xem mã giả của chương trình ta thấy, chương trình ngăn chặn việc debug sau dòng 35.

Vì vậy ta sẽ phân tích code. Đầu tiên gán v6 bằng chuỗi “AHi23DEADBEEFCOFFEE”, chuỗi ta nhập vào lưu vào s2, sau đó tính s1 và so sánh nếu s1 = s2 thì in ra "you succeed!!"

S1 được tính như sau:

s[0] = v6[0] ^2 = 0x43 (kí tự C)

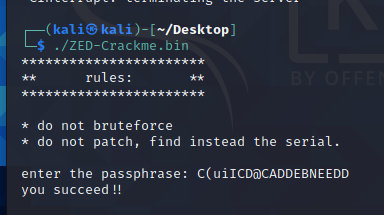
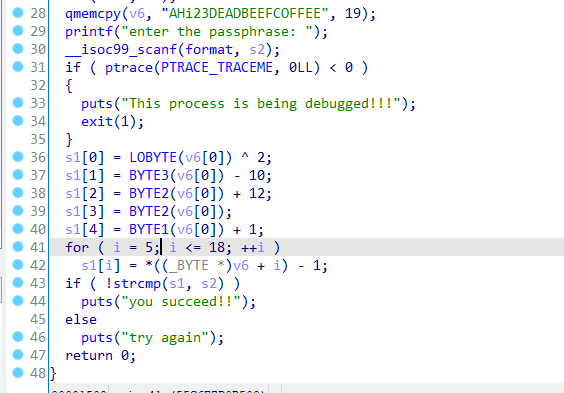
s[1] = v6[3] – 0xA = 0x28 (kí tự ()

s[2] = v6[2] + 0xC = 0x75 (kí tự u)

s[3] = v6[2] = 0x59 (kí tự i)

s[4] = v6[1] +1 = 0x49 (kí tự I)

Từ s[5] đến s[18] s[i]=v6[i]-1

Vậy chuỗi cần nhập là “C(uiICD@CADDEBNEEDD”

Kiểm tra: