TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM

KHOA CÔNG NGHỆ THÔNG TIN

Môn: Thực Hành Phân Tích Mã Độc

Họ Và Tên: Trần Hân Nhi

MSSV: 2011770131

Lớp: 20DATA1

Báo cáo tuần 4

```
13  i = 0;
14  v9 = malloc(48uLL);
15  write(0, "Welcome CNTT HUTECH\n", 0x15uLL);
16  ptr[0] = v9;
17  v11 = 1;
18  write(0, "enter -88 to exit HUTECH, -99 to get Lottery numbers.\n", 0x37uLL);
19  while ( 1 )
20  {
21    write(0, "You bet on any number(0-999): ", 0x1DuLL);
22    read(1, buf, 4uLL);
23    v8 = atoi(buf);
```

Ở thể thấy hàm i ban đầu đầu được khai báo bằng 0

v9 = malloc (48 byte)

Và ptr[0] được khai báo bằng v9

Các dòng 15 18 21 là các dòng để in ra màn hình

Trong while có read dùng để truyền giá trị đầu vào lần lượt là kiểu int là 1, void , và size

v8 = được khai báo băng atoi đây là 1 hàm dùng để ép kiểu dữ liệu

```
for ( i = rand() % 1000; i == v8; i = rand() % 100 )
  ;
if ( v8 == -88 )
  break;
if ( v8 == -99 )
{
  for ( j = 0; j < v11; ++j )
    free(ptr[j]);
  ptr[0] = malloc(0x30uLL);
  write(0, "Please give me 1 billion VND.\n", 0x1EuLL);
  v11 = 1;
}
else
{
  v7 = malloc(v8);
  *v7 = v11;
  ptr[v11++] = v7;
  if ( v11 == 10 )
  {
    write(0, "You are out of money.", 0x16uLL);
    return 0;
  }
}
snprintf(s, 0x32uLL, "%d", i);
write(0, "Today's number is: ", 0x14uLL);
write(0, s, 3uLL);
write(0, "\nWish you luck next time\n", 0x1AuLL);
if ( *v9 == 5 )
  HAHA();
```

Tiếp đến là các dòng if else

Đối với v8 được ép kiểu int từ trước sẽ có các trường hợp if như sau

Đối với if đầu là v8 == -88 khi nhập sẽ bị out khỏi chương trình

Đối với if v8 == -99 chương trình sẽ giải phóng bộ nhớ.

Trường hợp nếu nhập quá 10 sẽ bị out khỏi chương trình

Khi ta nhập đúng điều kiện của v9 = 5 thì cat file flag.txt trong biến HaHa và sẽ biết được flag

Nhập số nguyên bằng với số byte của v9 đang khai báo là n1 trong bộ nhớ. Khi nhập 5 lần n1 sẽ thỏa mã được điều kiện v9 ==5 nhưng nếu như thế thì có thể v9 đang giá trị n1 nên flag chưa xuất hiện

Tiếp theo thì ta sẽ nhập -99 để bắt đầu với điều kiện v8 == -99 vì hiện tại ở code cho thấy v7 = malloc(v8) → v7, v9 dùng chung một vị trí trong bộ nhớ có thể dùng điều này để bắt đầu lại 1 điều kiện khác

Khi giải phóng bộ nhớ ban đầu thì con trỏ sẽ trỏ đến vùng bộ nhớ mới và tiếp tục nhập 5 lần n1 đển thỏa điều kiện v9 == 5 và flag sẽ xuất hiện.