**MISC**

**Phân tích:**

Ngay ở phần đầu của ct chúng ta thấy phía sau fgets sẽ có các vòng lặp đếm số ký tự nhập vào thực hiện so sánh tại instruction: **cmp ecx, 21h**



từ đó chúng ta suy ra số ký tự nhập vào phải bằng 33(21h=33) ký tự.

Tiếp theo chúng ta sẽ gặp: các hàm api được gọi: **CreateFileA, GetFileSize, CreateFileMappingA, MapViewOfFile** dùng để nạp **quinquin.bmp** vào bộ nhớ .

tiếp tục chúng ta gặp vòng lặp :



chức năng biến ký tự chúng ta đã nhập thành 1 hoặc 0 bằng cách chia 2 và lấy dư

phân tích ta sẽ thấy mỗi ký tự chuyển về mã hex r chia theo các bước trên sẽ đc dãy 1,0 có độ dài 8 ký tự.

tiếp theo là:



đoạn mã này sẽ tạo ra các địa chỉ khác nhau gồm 264 địa chỉ để ghi các ký tự 1;0 trên kia vào vùng nhớ của file bmp đã nạp:



sau khi nạp hoàn tất việc khi hoàn tất việc ghi các file 1;0 bộ đệm đc nạp của bmp sẽ đc đổ vào file bmp và kêt thúc ct:



**Giải pháp:**

sau khi chạy xong chúng ta thử kiểm tra cái ảnh kia xem sao

dùng HxD để compare giữa file backup và file đã edit:



đúng là có sự khác biệt! và đặc biệt là tại các vị trí khác nhau thì ở file gốc đều là 0 hoặc 1, thử extract các chuỗi 1;0 đó xem có gì hay ho k.

quay lại tại đoạn ghi các số 1;0 vào vùng nhớ, tiến hành patch code lại để thay vì chuyển từ chuỗi 1;0 của chúng ta vào vùng nhớ thì chúng ta sẽ làm ngược lại:



cho chạy hết vòng lặp và chúng ta chỉ cần nhảy tới địa chỉ do chứa chuỗi 1;0 cũ do **eax+esi** trỏ tới là ta thu được chuỗi 1;0 từ file bmp;

chuỗi thu được:

011100101100110001110110001011000111011000010110001100101010111010001100010000101010111000001100110001100110101011001100110010100010110010101110001000101100110000101010000101100010110010011110101000101011011001001010000011000001001011110110011101100101110000010100

tổng cộng 264 ký tự.

bây h viết 1 code c để đổi mỗi 8 kí tự 1;0 thành mã hexa hoặc decimal của các kí tự ascii:

đây là code của mình :

#include<iostream>

#include<fstream>

using namespace std;

int main()

{

char a[7];

int t;

int b[7];

char v[] = { " " };

ifstream f1;

ofstream f2;

f1.open("E:\\x.txt", ios::in | ios::out);

f2.open("E:\\5.txt");

for(int j=1;j<=33;j++)

{

t = 0;

for (int i = 0; i <= 7; i++)

{

f1 >> a[i];

b[i] = a[i]-48;

}

cout << a << endl;

cout << b[1] << endl;

t = b[7];

for (int i = 6; i >= 0; i--)

t = t \* 2 + b[i];

f2 << t;

f2 << " ";

cout << t << endl;

}

f1.close();

f2.close();

cin.get();

return 0;

}

sau khi hoàn tất chuyển đổi thu được các mã dec:

78 51 110 52 110 104 76 117 49 66 117 48 99 86 51 83 52 117 68 51 84 104 52 121 69 109 82 48 72 111 110 58

đổi thành ascii:

**N3n4nhLu1Bu0cV3S4uD3Th4yEmR0Hon:(**