Hashes – Flare-on 2k17

Thấy anh em viết tâm sự rồi writeup mà cũng thấy xao xuyến quá. Thôi thì bớt chút lười ra để viết writeup cái bài mà mình kiếm được flag bằng cách mà người ta gọi là đoán mò =)), chắc một số người cũng làm ra bằng cách này  (dù rằng mình đã code cái đoạn code bruteforce rồi. Mịa nó code chạy lâu vãi. Thấy trên twiter của Tuấn Anh Nguyễn làm sau này bảo mất mười mấy tiếng mới ra ).

Oke.

Tính mình nhiều khi lười vãi nhái. Cái gì mà làm tay được là làm người ta gọi là " quay tay" . Đến bài vmcode mình còn làm bằng tay nữa là  Thế nên bài này sau một hồi debug thì thấy độ dài flag nó là 30 ký tự và chưa hiểu được thuật toán của nó buồn buồn ngồi đoán flag vì tahays từ lv1- lv6 flag nó có tý liên quan tới tên file, chuỗi trong file. Vậy nên nảy ra ý tưởng đoán flag ☺.

Quá trình đoán bắt đầu:

Thấy có chuỗi **"You have hashed the hashes!"** có vẻ liên quan.

@flare-on.com: 13 ký tự roài

CÒn thiếu 17 ký tự nữa, lần mò thấy : **hashed the hashes** đúng tròn 17 ký tự. Có nhẽ nào ra rồi nhưng đời ko như mơ hay là tại cái số vẫn nhọ từ trước tới giờ, thay thế số má, các ký tự đặc biệt mà

ko được ☹(. Nản quá. Nghĩ rằng đoán méo có khả thi rồi

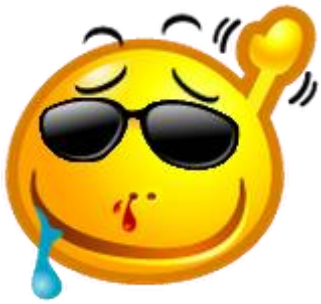
Quay lại ngồi đọc thuật toán với 1 hint của anh Merc ☹(sau đó ngồi hì hục lôi visual ra code bruteforce sau chờ thấy mịa nó hơn tiếng rồi mà mới được có một tý ko à. Biết bao giờ mới xong 1

block. Ngồi chửi thầm DKM bọn này chơi nhau à, brute éo gì lâu thế .
Bứt dứt khó chịu ngồi chờ code chạy sau đó lại bảo hay thử đoán phát nữa, đoán lần trước chắc hay bỏ qua cái gì. Reset lại đầu, mọi ký tự đoán lần trước xóa hết. Thế rồi ngồi đoán kết hợp xem lại mấy flag các lv trước ô la la thấy có vẻ có " Ánh sáng nơi cuối con đường rồi" mấy cái ký tự thần thành trong các flag cũ mình bỏ sót và trời quả ko phụ những thằng lười: thử với h4sh3dxxxxxxxxxxx @flare-on.com và thấy pass qua được block đầu tiên. Lúc đấy tâm trạng ko biết nói gì

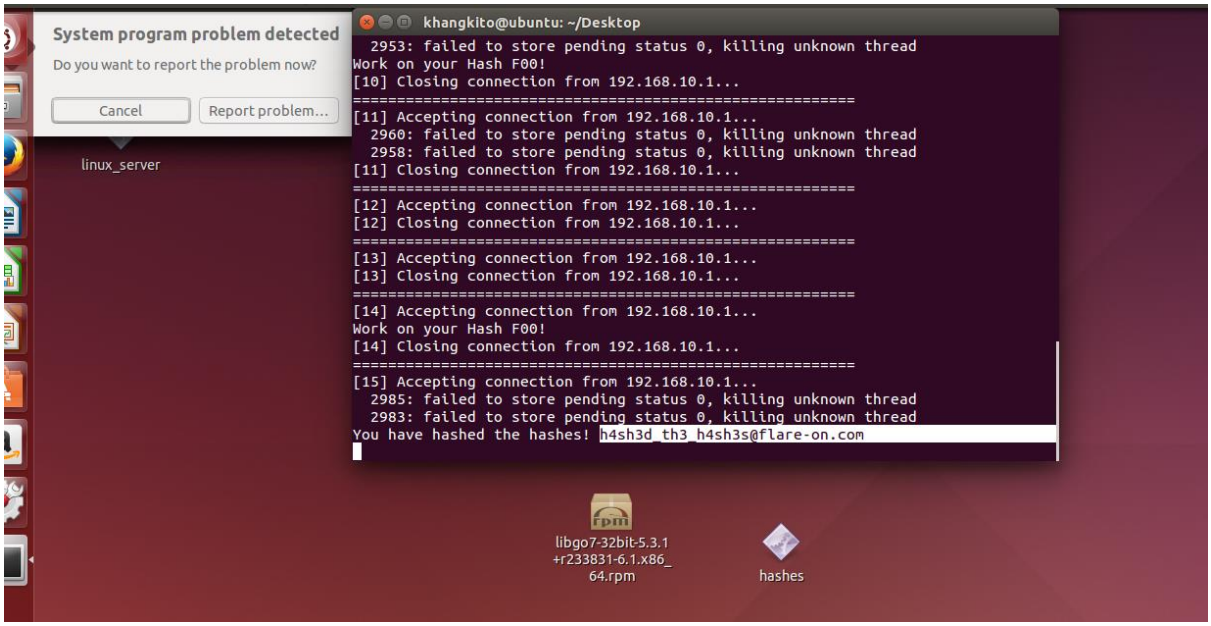
Thay vào cái thằng code khi đang chiếm dụng CPU con máy Alienware R 3 mới mua được nửa năm mua về mục đích chơi game thì ít mà chạy máy ảo thì nhiều thấy code

mình đúng cmnr Thật ko ngờ, nghĩ rằng bớt được 1 lần bruteforce, sau lại nhớ đến câu nói vẫn hay tự thầm thì với bản thân mình : có lần 1 thì sẽ có lần thứ 2,.. lần thứ n (ở

đây chỉ cần lần thứ 3 thoai). Và rồi méo còn gì để nói, áp dụng công phu đoán block đầu áp dụng với block thứ 2, 3 cái flag mà mấy ông ra đề làm khó bằng việc bruteforce đã



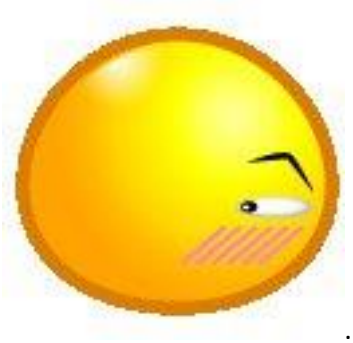
hiện nguyên hình . Và đây là kết quả



Còn cái chuỗi thần thánh đã giúp mình đoán đây:

```
.text:0804A326 add     dword ptr [ebp-24h], 1
.text:0804A32A
.text:0804A32A fail1:                                  ; CODE XREF: main_main+290↑j
.text:0804A32A mov     eax, [ebp-0C0h]
.text:0804A330 cmp     eax, [ebp-24h]
.text:0804A333 jg      loc_804A2AB
.text:0804A339 cmp     byte ptr [ebp-19h], 0
.text:0804A33D jz      fail
.text:0804A343 mov     eax, 1
.text:0804A348 mov     dword ptr [ebp-0D8h], offset aYouHaveHashedT ; "You have hashed the hashes!"
.text:0804A352 mov     dword ptr [ebp-0D4h], 1Bh
.text:0804A35C mov     esi, [ebp-0D8h]
.text:0804A362 mov     edi, [ebp-0D4h]
.text:0804A368 mov     [ebp-0D0h], esi
.text:0804A36E mov     [ebp-0CCh], edi
.text:0804A374 mov     ebx, ds:os_Args
.text:0804A37A mov     edx, ds:dword_805022C
.text:0804A380 cmp     edx, eax
.text:0804A382 jle     short loc_804A388
.text:0804A384 test    eax, eax
.text:0804A386 jns     short loc_804A397
```

Có lẽ bài này do mấy bác ra đề hơi chủ quan nên dễ đoán, dù gì phải công nhận mình may mắn VL


. Đỡ tổn hao con máy yêu quý

Thực ra viết bài này mục đích để khoe con máy của mình thôi chả có gì hay ho đâu ^_^