

In The

Name Of God

DeLTAHaCkiNgSecurityTEAM

موضوع: Crack

نویسنده : شاهین.ر (Vampire) ir.exploit0iter@yahoo.com

مقدمه: خوب بازم سلام با نام و یاد خدا شروع میکنیم!

برای اینکه در خواستهای بسیار زیادی در زمینه آموزش Crack از من شد به همین دلیل می خوام

به شما یاد بدم چطوری همیشه هر نرم افزاری یا ... رو Crack کرد!

اما خوبه بدونید اگر می خواهید واقعا یه Cracker بشید حتما باید :

۱- زبان Assembly رو فول باشد (هرچی بیشتر بلد باشی کر برات شیرین و راحت تره)

۲- آشنایی کامل با مهندسی معکوس

۳- توانایی جمع آموری اطلاعات

۴- توانای فهم و بررسی کد ها

۵- آشنایی کامل با Decompiler ها

۶- آشنایی کامل با Debugger ها

۷- برنامه نویسی با Assembly در ویندوز (آشنایی کامل API ها ...)

۸- برنامه نویسی به زبانهای دیگر

۹- از همه مهمتر پشت کار و علاقه (که جزو آموزش نیست چون همتون این ویژگی رو دارید)

البته به این زودی ها نگید بابا اگه می دونستیم این همه چیز می خواد بیخیال می شدیم

به مرور زمان اگه خدا بخواد همه رو دونه دونه براتون توضیح می دم

فعلا برای شروع با یم چیز خیلی خیلی ساده شروع می کنیم!

تنها چیز هایی هم که الان لازم داریم:

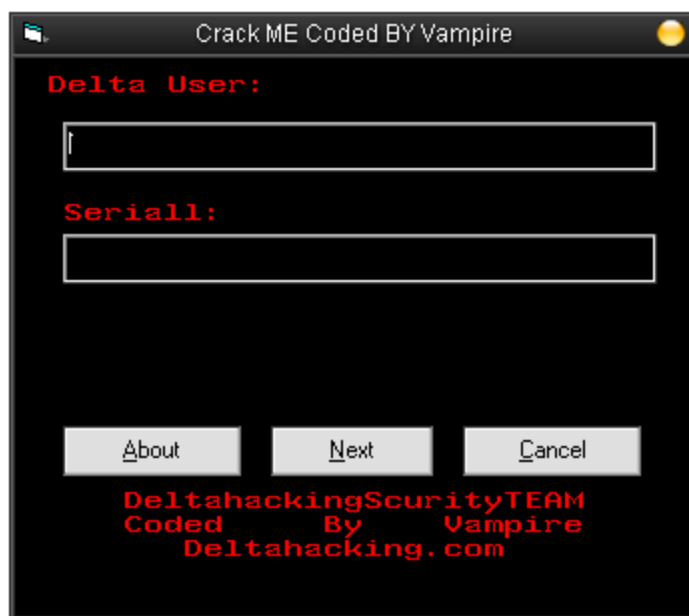
W32Dasm

Hacker view

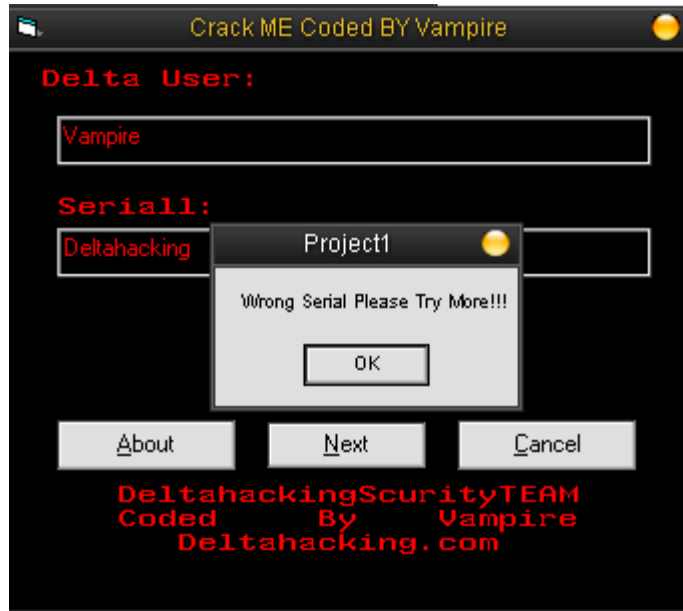
این برنامه رو راحت با یه **Search** تو **Google** پیدا میکنید!

برای شروع هم یه برنامه خیلی خیلی ساده با **Visual Basic 6.0** نوشتم که می
تونید **Crack** کنید!

چون دنبال **USER** و **PASS** می گرده !



حالا یه **U/P** مزخرف میدیم!



می بینید که **Error** میده و می گه **Serial** اشتباه است!

حالا ما باید متن پیام رو يك به خاطر بسپاریم.

حالا برنامه **W32Dasm** روی اجرا میکنیم!

حالا می پرسید اصلا این **W32Dasm** چی هست:

W32Dasm په **Disassembler** که و کارش تبدیل يك فایل اجرایی به زبان اسمبلی است!

حالا با استفاده از **Open The File To Disassemble**

فایل **CrackME** رو که ضمیمه کردم رو باز کنید!

بعد از منوی **Refs** گزینه **String Data References** انتخاب کنید.

حالا لیستی از متنهایی که در برنامه وجود دارد رو می بینید .

همون Error که قبلا حفظ کرده بودید بگردید!

حالا دوبار روش **Click** کنید کنید

حالا از این لیست خارج و به صفحه اصلی **W32Dasm** برید!

نکته: شما میتونید از منوی **Search** گزینه ی **Find Text** رو انتخاب کنید!

و بعد همون **error** رو اینجا **Search** کنید!

نکته: به حروف بزرگ و کوچک حساس است!

خوب حالا به همچین تصویری میبینید!

```
0040269E S1          push ecx
0040269F EB41          jmp 004026E2

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
| 0040265C(C)      آدرس مرجع
|
* Possible StringData Ref from Code Obj -> "Wrong Serial Please Try More!!!"
|
004026A1 C7459C701B4000   mov [ebp-64], 00401B70

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:004025D3(U)
|
004026A8 8D5594          lea edx, dword ptr [ebp-6C]
004026AB 8D4DD4          lea ecx, dword ptr [ebp-2C]
004026AE C7459408000000   mov [ebp-6C], 00000008
```

حالا **Error** رو تو تصویر می بینید.

حالا می پرسید اون یکی فلش چیه!

اون هاعداد آدرسه جایی هست که يك دستور شرطي برسي ميکند اگر U/P اشتباه يا درست بود چه پیغامی رو نشون بده!

خوب ببینید به طور کامل به این صورت می شه که :

فرض کنید برنامه ای نوشتیم که از ما اسم یا یوزر یا هر چیزی رو می خواد حالا مثلا ما اگه یوزر Vampire

رو بدید يك پیغام بده بگه Hi Vampire و در غیر این صورت پیغام بده
WRONG USER یا هر چیزی دیگری

حالا بنا به توضیحی که دادم دستور شرطي ما اینطوری شده:

```
if User = Vampire  
Hi Vampire  
else  
Wrong USER
```

(البته این طریقه استفاده از دستور شرطي کامل نیس و فقط برای فهم بهتر شماست
(.....)

بعد اگه دستور شرطي رو بر عکس کنیم همونطور که فهمیدید وقتی بله وقتی ما یوزر

Vampire رو بدیم به ما میگه Wrong User و اگر یوزر دیگری بدیم میگه Hi Vampire

خوب شما برای Crack کردن دقیقاً همین کار رو انجام میدید یعنی با تغییر دستور اون کدی که میخواهید رو اجرا می کنید

همونطور گفتم اون اعداد در واقع آدرس جایی هست که این دستور شرطی قرار در اون اونجا قرار داده

بعد به اون آدرس میرید با دوبار Click راست ماوس روی اون اعداد که مشخص کردم!

به آدرس مورد نظر می رسیم. به این صورت که در تصویر می بینید!

```
02659 8945C4      mov dword ptr [ebp-3C], eax
0265C 7443          je 0040107C
0265E 8D5594      lea edx, dword ptr [ebp-6C]
02661 8D4DD4      lea ecx, dword ptr [ebp-2C]
ssible StringData Ref from Code Obj ->"OK. You Good Cracker"
02664 C7459C401B4000  mov [ebp-64], 00401B40
0266B C7459408000000  mov [ebp-6C], 00000008
ference To: MSVBVM60.__vbaVarDup, Ord:0000h
02672 FF157C104000  Call dword ptr [0040107C]
02678 8D45A4      lea eax, dword ptr [ebp-5C]
0267B 8D4DB4      lea ecx, dword ptr [ebp-4C]
0267E 50          push eax
0267F 8D55C4      lea edx, dword ptr [ebp-3C]
```

خوب دستور اینجا JE هست یعنی اگر کدی که دادیم درست نبود به آدرسی که جلوی این دستور هست برو

یادتون نره دستور JE یکی از دستورهایی شرطی زبان اسمبلی هست

که مخالف اون می شه **JNE (JUMP IF NOT EQUAL)**

بعد قبل از اینکه دستور رو تغییر بدیم

به شماره ای که در پایین برنامه **W32Dasm** وجود داره نیاز داریم یه راه راحت تر هم هست

که بعدا براتون میگم !

به این تصویر نگاه کنید!

Code Data @:0040265C @Offset 0001265C in File:Vampire.exe

خوب همونطوری که در تصویر نشون دادم این **Offset** مربوط می شه

به اون دستور یعنی **JE** حالا میگرد این به چه درد می خوره

اگه دوست داید بدونین این اعداد از کجا آمده

به تصویر قبلی که دستور **JE** رو نشون دادم!

دقت کنید این کدا رو میبینید:

:0040265C 7443 JE 004026A1

عدد **265C** این یعنی جایی که این دستور قرار داره

این اعداد رو به خاطر بسپارید!

بعد حالا برنامه **Hacker View** باز میکنیم! و به مسیر فایل **Vampire.exe** برین و بازش کنید.

ضمنا با استفاده از کلید های **Alt+F2** می تونید درایو رو نیز عوض کنید!

بعد باز کردن Vampire.exe در Hacker View با زدن

دکمه F4 منویی میاد که از داخلش Decode رو انتخاب می کنیم

حالا کلید F5 رو بزنی تا اون شماره که حفظ کردید رو در اینجا Serach کنید.

خوب F5 رو بزنی 265C را تایپ و Enter بزنی تا پیدا شود.

حالا به همچین چیزی می بینید!

```
UAMPIRE.EXE ↓FRO PE.0040265C a32 ----- 20480 || Hie
.0040265C: 7443 این باید تعقیب کته je .0004026A1
.0040265E: 8D5594 lea edx,[ebp]-0
.00402661: 8D4DD4 lea ecx,[ebp]-0
.00402664: C7459C401B4000 mov d,[ebp]-006
.0040266B: C7459408000000 mov d,[ebp]-006
.00402672: FF157C104000 call _vbaUardup
.00402678: 8D45A4 lea eax,[ebp]-0
.0040267B: 8D4DB4 lea ecx,[ebp]-0
.0040267E: 50 push eax
.0040267F: 8D55C4 lea edx,[ebp]-0
.00402682: 51 push ecx
.00402683: 52 push edx
.00402684: 8D45D4 lea eax,[ebp]-0
.00402687: 53 push ebx
.00402688: 50 push eax
.00402689: FF151C104000 call MSUBUM60.595
.0040268F: 8D4DA4 lea ecx,[ebp]-0
.00402692: 8D55B4 lea edx,[ebp]-0
.00402695: 51 push ecx
.00402696: 8D45C4 lea eax,[ebp]-0
.00402699: 52 push edx
.0040269A: 8D4DD4 lea ecx,[ebp]-0
```

یادتون نره در اسمبلی دستورات بجز کد اسمبلی مثلا JE يك کد بصورت

هگز هم دارن که برای همین دستور ۷۴ هست.

همونطور که قبلا گفتم باید ما این شرط رو برعکس کنیم یعنی از JE به JNE تغییر بدیم!

کد هگز برای JE عدد ۷۵ هست. پس ۷۴ رو به ۷۵ تغییر بدید!

برای Edit کلید F3 رو میزنید حالا ۷۵ رو تایپ میکنیم!

```
UAMPIRE.EXE ↓FWO PE 0000265E a32 <Editor> 20480 ||
0000265C: 7543 به این صورت همیشه jne 0000026A1
0000265E: 8D5594 lea edx,[ebp]
00002661: 8D4DD4 lea ecx,[ebp]
00002664: C7459C401B4000 mov d,[ebp]-4
0000266B: C7459408000000 mov d,[ebp]-8
00002672: FF157C104000 call d,[0004010]
00002678: 8D45A4 lea eax,[ebp]
0000267B: 8D4DB4 lea ecx,[ebp]
0000267E: 50 push eax
0000267F: 8D55C4 lea edx,[ebp]
00002682: 51 push ecx
00002683: 52 push edx
00002684: 8D45D4 lea eax,[ebp]
00002687: 53 push ebx
00002688: 50 push eax
00002689: FF151C104000 call d,[0004010]
0000268F: 8D4DA4 lea ecx,[ebp]
00002692: 8D55B4 lea edx,[ebp]
00002695: 51 push ecx
00002696: 8D45C4 lea eax,[ebp]
00002699: 52 push edx
0000269A: 8D4DD4 lea ecx,[ebp]
0000269D: 50 push eax
```

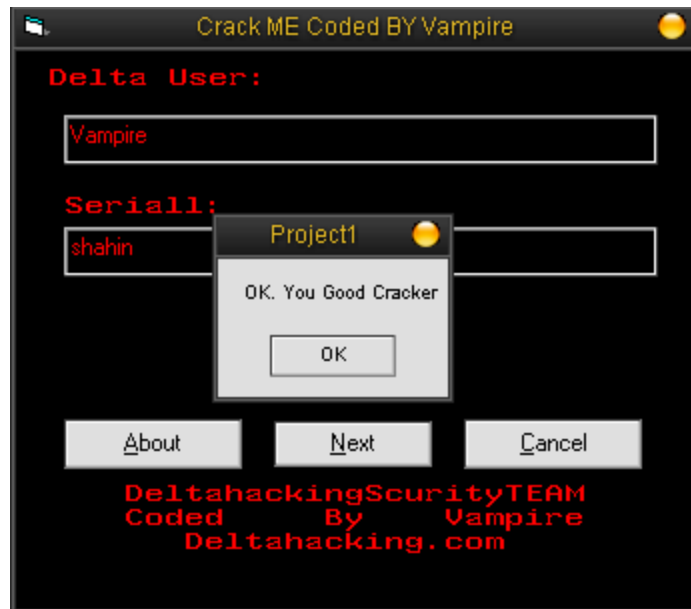
و برای ذخیره کردن کلید F9 را می زنیم.

البته می تونید یه کار راحت تر هم بکنید اول F3 و بعد F2 می زنید!

و حالا با آرامش JE رو JNE تغییر بدید!

حالا با کلید Esc یا F10 از Hiew خارج شید!

حالا با آرامش Vampire.exe رو باز کنید و یه U/P از خودتون بدید!



هه هه هه شما اولین نرم افزار رو Crack کردید!

البته این روش مال عصر دایناسورهاست اما انجامش لذت بخش و یاد گیریش لازم بود!

امید وارم هر جا که هستید موفق و سرحال و پیروز و خوش و خرم باشید!

با تشکر Vampire

Special Thanks TO my Best friends X_f_t_x,D_7J

M@s0oD H!V,Hessamx,

AND TK

deltahacking.com

deltahacking.net

The End

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.