

Target: crackme v2.0 by Crucehead/MiB
Lang. : masm32
Tools : Lloyd , Pied
Cracker: allko

Learn Reverse Engineering Series- lesson seven code injection (II)

Introduction:

لم أكن أتوقع الوصول إلى الدرس السابع بهذه السرعة... سلسلة تعلم الهندسة العكسية لم تبدأ إلا منذ شهر أو أكثر تقريبا... على كل حال أرجو أن تكونوا قد استفدتم من الدروس... درس اليوم يعتبر تطبيقا جيدا على code injection .. لن أطيل عليكم دعونا نبدأ.

Get The Party Started :

الهدف لهذا اليوم ليس غريبا عليكم... كنا قد فككنا حمايته في الدرس الثالث (allko 0010) لذا قبل البدء راجع الدرس لأنني لن أعيد شرحه من جديد... حسنا دعني أذكرك بالخطوات الواجب عملها لتطبيق الـ code injection :

- 1- إيجاد نقطة لتغيير الـ code-flow (سريان الأوامر).
- 2- إيجاد الـ cave المناسب لوضع الكود فيه.
- 3- إرجاع السيطرة للبرنامج.

الحماية تتلخص في مكان واحد فقط... من 401261 وحتى أمر RETN ... إذن مبدئيا سنستبدل هذه الـ procedure بأخرى... انقر على أول أمر على عنوان 401261 وانظر إلى قسم التعليقات... Local call from 0040117D أها... إذن اذهب إلى 40117D وغير الأمر إلى... لحظة.. قبل هذا دعنا نجد الـ cave المناسب... كما ترى ففي نهاية البرنامج فراغ كبير جدا (لهذا أحب برامج الاسمبلي:) اختر أي عنوان وليكن 401470 إذن غير أمر CALL Crackme2.00401261 إلى CALL Crackme2.00401470 ... الآن لنرجع إلى 401261...

```
00401261  $ A1 60204000 MOV EAX,DWORD PTR DS:[402060]
00401266  . 3905 64204001 CMP DWORD PTR DS:[402064],EAX
0040126C  . 75 2F         JNZ SHORT Crackme2.0040129D
0040126E  . 33C0         XOR EAX,EAX
00401270  . 8B7C24 04    MOV EDI,DWORD PTR SS:[ESP+4]
00401274  . 8B7424 08    MOV ESI,DWORD PTR SS:[ESP+8]
00401278  > 0FB61F      MOVZX EBX,BYTE PTR DS:[EDI]
0040127B  . 0FB616      MOVZX EDX,BYTE PTR DS:[ESI]
0040127E  . 80FA 30     CMP DL,30
00401281  . 7C 1A      JL SHORT Crackme2.0040129D
00401283  . 80FA 39     CMP DL,39
00401286  . 7F 15      JG SHORT Crackme2.0040129D
00401288  . 80EA 30     SUB DL,30
0040128B  . 83E3 0F     AND EBX,0F
0040128E  . D0EB       SHR BL,1
00401290  . 2ADA       SUB BL,DL
00401292  . 75 09      JNZ SHORT Crackme2.0040129D
00401294  . 47         INC EDI
00401295  . 46         INC ESI
00401296  . 803F 00     CMP BYTE PTR DS:[EDI],0
00401299  . 75 D0      JNZ SHORT Crackme2.00401278
0040129B  . EB 04      JMP SHORT Crackme2.004012A1
0040129D  > 33C0         XOR EAX,EAX
0040129F  . EB 05      JMP SHORT Crackme2.004012A6
004012A1  > B8 01000000 MOV EAX,1
004012A6  > C3         RETN
```

لا اعتقد إن نسخ الكود كما هو يعتبر أمر جيدا... دقق النظر قليلا... ضع نقطة توقف عند **401261** وتتبع F8 (أو بكل بساطة راجع الدرس الثالث!!) بداية هناك عملية مقارنة... يجب إن يكون طول الـ username مساويا للسيرال... ثم يتم وضع اليوزرنيم في EDI والسيرال في ESI... لكن نحن نريد إن يتم تشفير اليوزرنيم لإنتاج الكلمة الصحيحة... لا نريد عمل أي شيء للسيرال الذي أدخلناه... إذن فان أمر mov على عنوان **401274** سيحذف من الكود... وبالتالي سنحذف 40127B أيضا... هناك أوامر للتحقق من أن

السيريال رقم...سنحذفها جميعها (بدئا بـ 40127E وحتى 401288) أي إن كل عملية تتعلق بـ DL (أي بالسيريال) لا نريدها...أيضا سنحذف 401290 و 401292 .(عملينا مقارنة... غير لازمتين)

والآن استخدم الـ plug in المرفقة (إن كنت لا تعلم كيفية استخدامها فانظر إلى الملاحظات بالأسفل)
الآن حدد جميع هذه الأوامر واضغط باليمين واختر Asm2Clipboard ثم cope fixed asm code to clipboard وافتح الـ notepad والصق الكود ثم احذف الأسطر التي ذكرتها...
الآن ما لدينا هو التالي...كود يستقبل الـيوزرنيم ويقوم بتشفيره و...فقط!!! إذن نحن نريد تخزين الكود في مكان ما كي نظهره للمستخدم...راجع الدرس الثالث لتعلم إن السيريال يطرح منه 30 ثم يقارن مع الـيوزرنيم المشفر...إذن يجب إن نضيف 30 إلى الكود المشفر...ونخزنه في مكان ما...
فلنختر بداية مكانا لتخزين النتيجة فيه...انظر بالأسفل إلى قسم الـ data وابحث عن مكان فارغ مناسب...هناك العديد من الأماكن وليكن 4021B1 (أعيد واذكر بأنه يمكنك اختيار أي مكان آخر) إذن يلزمنا أمر add bl,30 وأمر mov byte ptr [4021B1],bl لاحظ كلمة byte ptr إن ptr هي اختصار لـ pointer أي مؤشر....أي إننا نريد مؤشر يشر إلى بايت...لأن الكود مكون من أرقام كل منها بجم بايت...

لكن انتظر لو تركنا الأمر هكذا سيخزن الرقم الأول في 4021B1 ثم في الدورة الثانية سيخزن الرقم الثاني فوفقه!! إذن يلزمنا عداد وحيث إن esi غير مستخدم في هذا الكود (كان يستخدم للسيريال قبل أن نحذفه) إذن سنستخدمه ليصبح الأمر هكذا mov byte ptr [4021B1+esi] لكن... ماذا لو كان esi يحتوي على قيمة ما عند وصولنا للكود؟ إذن يجب إن نصفره قبل استخدامه...يلزمنا أمر xor esi,esi لكن أين سنضعه؟ يجب إن نضعه خارج الـ loop الداخلية (فكر جيدا...لو وضعناه في الـ loop الداخلية فانه في كل دورة سوف يتم تصفير esi ثم يعد لـ 1 ومن ثم يتم تصفيره ثم يعد لـ 1 وهكذا...أي انه لم يعد يؤدي وظيفته)...فلنضعه مثلا عند العنوان 40127B...يلزمنا أيضا أمر inc esi لكن لحسن الحظ هذا الأمر موجود أصلا...والآن بعد أن قمنا بالحذف والإضافة غير عناوين القفزات كما تعلمت... (أي انظر إلى كل قفزة في الكود الأصلي إلى أين تقفز ثم غير العنوان بناء على ذلك) إذن أصبح الكود بالشكل التالي:

00401470	A1 60204000	MOV EAX,DWORD PTR DS:[402060]
00401475	3905 64204000	CMP DWORD PTR DS:[402064],EAX
0040147B	75 22	JNZ SHORT cracked.0040149F
0040147D	33C0	XOR EAX,EAX
0040147F	8B7C24 04	MOV EDI,DWORD PTR SS:[ESP+4]
00401483	33F6	XOR ESI,ESI
00401485	0FB61F	MOVZX EBX, BYTE PTR DS:[EDI]
00401488	87E3 0F	AND EBX,0F
0040148B	0000 00	SHR BL,1
0040148D	0000 00	ADD BL,30
00401490	889E B1214000	MOV BYTE PTR DS:[ESI+4021B1],BL
00401496	47	INC EDI
00401497	46	INC ESI
00401498	803F 00	CMP BYTE PTR DS:[EDI],0
0040149B	75 E8	JNZ SHORT cracked.00401485
0040149D	EB 04	JMP SHORT cracked.004014A3
0040149F	33C0	XOR EAX,EAX
004014A1	EB 05	JMP SHORT cracked.004014A8
004014A3	B8 01000000	MOV EAX,1
004014A8	C3	RETN

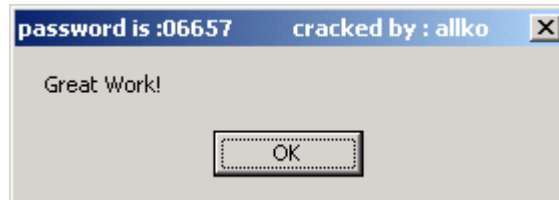
والآن قم بحفظ التغييرات وأعد التشغيل... (بعد إعادة التشغيل ستظهر صورة الكود كما بالأعلى)
لقد أظهر لنا رسالة good boy إذن فقد نجحت المهمة... لكن انتظر أليس من المفروض إظهار السيريال للمستخدم؟ حسنا ، ما رأيك بإظهاره في نفس رسالة good boy ؟ اذهب إلى تلك الرسالة...

00401186	BB 8A204000	MOV EBX,Crackme2.0040208A	ASCII "Great Work!"
0040118B	EB 05	JMP SHORT Crackme2.00401192	
0040118D	BB 71204000	MOV EBX,Crackme2.00402071	ASCII "Nope, but keep trying :
00401192	6A 00	PUSH 0	Style = MB_OK+MB_APPLMODAL
00401194	68 68204000	PUSH Crackme2.00402068	Title = "CrackMe2"
00401199	53	PUSH EBX	Text
0040119A	FF75 08	PUSH DWORD PTR SS:[EBP+8]	hOwner
0040119D	E8 9B020000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA

لاحظ إن رسالتي good boy و bad boy هما في الواقع رسالة واحدة لكن هناك 2 strings إذن يمكننا عمل التالي...تغيير Great Work إلى عنوان السيريال الصحيح أي 4021B1...وهناك حل آخر بتغيير عنوان الرسالة بدلا من تغيير النص...أي تغيير title وذلك بتغيير أمر PUSH 40206B إلى PUSH 4021B1...يمكننا أيضا عمل بعض التغييرات كإضافة جملة ***: The password is cracked by allko إذن أنا سأختار الطريقة الثانية (هناك طرق أخرى كثيرة...)

004021A0	54	68	65	20	70	61	73	73	77	6F	72	64	20	69	73	20	The password is
004021B0	3A	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	:
004021C0	63	72	61	63	6B	65	64	20	62	79	20	3A	20	61	6C	6C	cracked by : all
004021D0	6B	6F	20	00	00	00	00	00	00	00	00	00	00	00	00	00	ko
004021E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

لاحظ أن الجملة التي أضفتها تقع قبل وبعد العنوان 4021B1 أي عنوان كلمة السر لنحصل على الشاشة الظاهر بالأسفل. لاحظ أيضا أنني تركت فراغا كبيرا نسبيا للباسورد فانا لا اعلم طول اليوزرنيم الذي سيدخله المستخدم (تذكر أن طول الباسورد = طول اليوزرنيم) لذا تركت 15 فراغ (لـ 15 حرف)...لو ادخل المستخدم اسما من 16 حرف سيستبدل حرف c في كلمة cracked ويحل محلها الرقم الأخير في السيرال...والآن بعد أن حفظت كل التغييرات وأدخلت allko كـيوزرنيم حصلت على التالي :



عظيم أليس كذلك؟

Do you know ?

ما الفرق بين المملكة المتحدة و بريطانيا و انجلترا ؟

المملكة المتحدة (United Kingdom) :
اسمها رسميا Great Britain and Northern Ireland وكما هو واضح من الاسم ، فهاتان الكلمتان (United Kingdom) تطلقان على بريطانيا وايرلندا الشمالية معا.
بريطانيا (Great Britain) :
تطلق فقط على جزيرة بريطانيا -التي لا تشمل ايرلندا الشمالية - وتتكون بريطانيا من عدة أجزاء هي انجلترا (الأكبر وتحتل الجزء الشرقي والجنوبي من الجزيرة) واسكتلندا (الجزء الشمالي) وويلز (الجزء الغربي).
انجلترا (England) :
كما ذكرنا هي جزء من بريطانيا.

Outroduction :

That was completely wonderful , wasn't it? I think this is my – and your – real beginning in reverse engineering . But you should be prepared to a harder targets in the next examples...you should have a basic knowledge in PE files because it's very important... Again , feel free to contact me :

allko34/at@hotmail.com

Notes :

To use the accompanied plug in , simply copy it and paste it in olly folder , then when you lunch the program you could find it in "plug ins" menu or simply when you right click a line or more. Have fun.

Thx:

DiDi

for being a real friend, when everybody left me alone...thank you.

Xacker

For being a real master and teacher...thanks.

Dahaka

For your useful suggestions and comments..a lot of thanks.

22/2/2006 10:45 pm

There are many crackers, but only one allko
allko34@hotmail.com