



## Reverse Engineering Tutorials Series

**Simple Patching** 



## **Haboob Team**



بالتدارحم أأرحيم

الهندسة العكسية مجال واسع وهذا الدرس مقدّم للمبتدئين حيث سيتم شرح عملية ترقيع البرامج "patching" لتخطي السيريال نمبر الخاص بالبرنامج.

قبل البدء نحتاج للبرنامج التالي: "Olly Debugger" او اي برنامج آخر يقوم بنفس الطريقة

أيضاً قبل البدء, يلزم القارئ الحصول على نبذه بسيطه في لغة الاسمبلي وآلية عمل الستاك "Stack" اذاكان الهدف الإلمام بالهندسة العكسية اما اذاكان الهدف للتطبيق فقط فلا يلزم, حيث يمكن تطبيق الدرس بدون الإلمام.



تم عمل برنامج بسيط يطلب كود لتفعيل السريال نمبر بلغة السي لتطبيق الشرح, حيث يضهر البرنامج رسالة خطاً عند ادخال رقم السريال الخاطي ويتم اغلاق البرنامج ورسالة صحيحة عند ادخال الرقم الصحيح.

C:\Users\PC\Desktop\CrackMe.exe						
Enter the Key:123			<u>^</u>			
	Haboob 🔀					
	Invalid KEY					
	ОК					
			<b>T</b>			

نقوم بفتح ملف الـ exe ببرنامج الـ "Olly Debugger" عن طريق الخيارات او بالضغط على مفتاح F3. بعد فتح الملف ببرنامج الـ Olly نقوم بالضغط على زر تشغيل البرنامج او بالضغط على مفتاح F9 ( لمرة واحدة فقط )

بعد ذلك نقوم بالضغط على الزر الايمن في المساحة اليسرى (المساحة الخاصة بالديساسمبلر "Disassembler") ومن ثم اختيار [Search for ➔ All referenced text Strings] كما هو موضح في الصورة.



🔆 OllyDbg - CrackMe.exe - [CPU - main thread, module CrackMe]							• <b>×</b>			
C File View Debug Plugins Options Window Help								- 8 ×		
00C01312 00C01317	\$ E8 6D0200	100 CA FF JM	ALL CrackMe.000 1P CrackMe.0000	01584 011A3 -		🔺 Regi	sters	(FPU) <	< <	< <
00C0131C 00C0131D	. 55 . 8BEC	PU	JSH EBP DV EBP,ESP		Backup	+	1000	000 312 CrackMe.(ModuleEntruPoint)		
00C0131F 00C01322	. 8845 08 . 56	PU	JV EAX,DWORD PI JSH ESI DU ECY DWORD PI	TR SS: LEBP+	Сору	+	FDE 041F	000 BCC		
00C01325 00C01326 00C01328	. 03C8 . 0FB741 14	AD	D ECX,EAX	TR DS: LECX	Binary	+	041F	BD4 000		
00C0132C 00C0132F	. 8D51 18 . 03D0	LE	A EDX,DWORD P1 DD EDX,EAX	TR DS: LECX+	Assemble	Space	000e	812 CrackMe. <moduleentrypoint></moduleentrypoint>		
00C01331 00C01335	. 0FB741 06 . 6BF0 28		JVZX EAX,WORD F 1UL ESI,EAX,28 )D ESI EDV	TR DS:LECX	Label		IS 0	02B 32bit 0(FFFFFFF) 023 32bit 0(FFFFFFFF)		
00C0133A 00C0133C	. 3BD6 .~74 19		1P EDX,ESI E SHORT CrackMe	.00001357	Comment	;	IS P	02B 32bit 0(FFFFFFF) 02B 32bit 0(FFFFFFF) 052 32bit 2555		
00C0133E 00C01341	. 884D 0C > 384A 0C		OV ECX,DWORD PI	TR SS: LEBP+	Breakpoint		as e	02B 32bit 0(FFFFFFF)		
00C01344 00C01346 00C01349	. 8842 08 . 0342 00	M H	10V EAX,DWORD F 10D EAX.DWORD F	PTR DS: CEDX	Hit trace	+	Last	Err ERROR_ACCESS_DENIED (00000005) 246 (NO.NB.E.BE.NS.PE.GE.LE)		
00C0134C 00C0134E	. 38C8 .~72 0C	ġ	MP ECX,EAX JB SHORT Crack1	1e.00C0135C	Run trace		npty	0.0 0.0		
00C01350 00C01353	> 83C2 28	6	NDD EDX,28 MP EDX,ESI			_	npty npty	0.0 0.0		
Address	Hex dump	Data		Comment	Follow	Enter	D0	75EC343D RETURN to kernel32.75EC34	3D	-
00C1D000 00C1D000					Go to	•	1D4 1D8	0041FC14 773E9832 RETURN to ntdll.773E9832		
00C1D000 00C1D000					Follow in Dump	+	EØ	746AADB7 00000000		
00C1D000 00C1D000					View call tree	Ctrl+K	E8	00000000 7EFDE000		
00C1D000 00C1D000					Search for	۰.		Name (label) in current module	Ctrl+N	
00C1D000 00C1D000 00C1D000					Find references to	Þ		Name in all modules		
00C1D000 00C1D000					View	+		Command	Ctrl+F	
00C1D000 00C1D000					Copy to executable	•		Sequence of commands	Ctrl+S	77056
00C1D000 00C1D000					Analysis	+		Constant		L. TTOES
00C1D000 00C1D000					Bookmark	•		Binary string	Ctrl+B	
00C1D000 00C1D000					Dump debugged process					
00C1D000 00C1D000					Dump process (OllyDumpEx)			All intermodular calls		
Program er	tru point				process (only onlines)			All commands		Paused
r rogram er	NJ POIN				Appearance	+		All sequences		adou
								All constants		
								All switches		1
								All referenced text strings		
								User-defined label		
								User-defined comment		

عند اختيار الخيار اعلاه سيتم الوصول الى الصفحة الخاصة بالنصوص "Strings" نقوم بالضغط على الزر الأيمن واختيار "Search for text" ثم نبحث عن رسالة الخطأ التي ظهرت عند ادخال رقم السيريال الخاطئ في أول صورة بالشرح وهي "Invalid KEY"





بعد البحث وايجاد النص يتم الضغط مرتين عليه ليتم نقلنا الى نافذة الديساسمبلر "Disassembler" كما في الصورة التالية

🔆 OllyDbg - CrackMe.exe - [CPU - main thread, module CrackMe]						
C File View Debug Plugins Options Window Help	- 8 ×					
► ( × ) II + + + + + + + + + + + + + + + + +	K B R S 🗄 📰 ?					
116C1086       CC       INT3         116C1086       SBEC       PUSH ECX         116C1087       SBEC       PUSH ECX         116C1087       SBEC       PUSH ECX         116C1087       SBEC       PUSH ECX         116C1087       SBESC       PUSH ECX         116C1087       SB045 FC       CPLL CrackHe.010DB668       RSCII "Ente         116C1087       SB045 FC       CPLL CrackHe.010C1059       Reg2         116C1087       SB7 ESEPFFF       CRL CrackHe.010C1059       Reg1 = 018         116C1087       SB7 ESEPFFF       CRL CrackHe.010C1059       CrackHe.08C         116C1087       SBT ESEPFFF       CRL CrackHe.010C1050       CrackHe.010C1050         116C1087       SBT ESEPFFFF       CRL CrackHe.010DB67C       Text = "Core         116C1086       SBESE       PUSH CrackHe.010DB684       Text = "Core         116C1087       SBESE       PUSH CrackHe.010DB69C       Text = "Core         116C1086       SBESE       PUSH CrackHe.010DB69C       Text = "Core	<pre></pre>					
Address Hex dump Data Comment	▲ 0030FE44 75EC343D RETURN to kernel32.75EC343D ▲					
1141.0489           1141.0489 <td< th=""><th>0030FE64         0030FE64           0030FE64         77259382           0030FE64         77259382           0030FE64         74F9183           0030FE64         00000000           0030FE70         00000000           0030FE74         00000000           0030FE74         00000000           0030FE74         00000000           0030FE75         00000000           0030FE74         00000000           0030FE74         00000000           0030FE75         00000000           0030FE76         00000000<!--</th--></th></td<>	0030FE64         0030FE64           0030FE64         77259382           0030FE64         77259382           0030FE64         74F9183           0030FE64         00000000           0030FE70         00000000           0030FE74         00000000           0030FE74         00000000           0030FE74         00000000           0030FE75         00000000           0030FE74         00000000           0030FE74         00000000           0030FE75         00000000           0030FE76         00000000 </th					



هنا نصل الى المهم, الحدود في اللون الازرق تسمى إطار الستاك "Stack Frame" وهذا مايهمّنا لعمل الترقيع للبرنامج.



في الصورة اعلاه تم الضغط على زر الـ F2 لعمل نقطة كسر "Break Point" على بعض العمليات كما هو موضّح في اللون الأحمر في الصورة وتعني (عندما نقوم بتشغيل البرنامج يتم ايقاف البرنامج عند الوصول لأي عملية باللون باللون الأحمرالى ان يتم تشغيل البرنامج مرة أخرى بالضغط على زر F9, وهنا لن يتم التطرّق لجميع العمليات او بمصطلح آخر الأوامر (Instructions) في إطار الستاك "Stack Frame" وماتعنيه لأن الشرح خاص بالمبتدئين ونكتفي بالعمليات التي وضعنا عليها نقطة كسر "Break Point" (الموضحة باللون الأحمر على اليسار في الصورة اعلاه)



نقوم بعد تحديد العناوين والضغط على زر الـ F2 لتصبح باللون الأحمر بضغط زر التشغيل في القائمة باللون الازرق او ضغط زر الـ F9 الى ان يتم تغير اللون الاحمر للأسود كما في الصورة التالية عند هذا العنوان 00121090 وكما نلاحظ في اسفل الشاشة يمين باللون الأصفر ان البرنامج متوقف (Paused).

🔆 OllyDbg - CrackMe.exe - [CPU - main thread, module CrackMe]							
C File View Debug Plugins Options Window Help							
	+ LEMTWHC/KBRS	₩ ?					
Bit Allocation         F5         S5         PUSH EBP           00121091         51         88EC         HOU EBP, ESP           00121091         51         88ES         PUSH ECX           00121092         53         882FFFFF         CRLL CrackHe.00           00121091         53         78861300         PUSH ECX           00121092         E832FFFFF         CRLL CrackHe.00           00121091         593 72861300         PUSH ErackHe.00           00121097         E8 A4FFFFF         CRLL CrackHe.00           00121097         E8 A4FF15         OBCL 1000 PTR           00121002         F5 38451300         PUSH CrackHe.00           00121001         CRL B431300         PUSH CrackHe.00           00121002         S8 9CB61300         PUSH CrackHe.00           00121001         CR< B451300         PUSH CrackHe.00           00121001         CR< B451300         PUSH CrackHe.00           00121002         S8 56         PUSH	0138668 1012020 178 SS: CEBP-4J 10138678     ASCII "Enter the Key:"       0138678     Proj = 00138678 ASCII "Z CrackHe.00251050       0138670     Proj = 00138678 ASCII "Z CrackHe.00251050       01386870     Stule = MB_OK: HB_APPLM0D Title = "Haboob"       0138684     Proj = 00138678 ASCII "Z CrackHe.00251050       0138684     Text = "Congrast VALID House = NULL       0138690     Text = "Invalid KEV" HessageBoxA       0138690     Text = "Invalid KEV" HessageBoxA	Registers (FPU)         < < < < < < < < < <           FRX: 0051EE00          < < < < < < < < < < < < < < < < < < <					
Hddress Hex dump Data	Comment	0024FE60 00000001 0024FE60 00000001 0024FE64 0051959					
Bell Suberge         Bell Suberge		0022FE68         0021FE68         0051EE00           0022FE78         00000000         0020FE74         00000000           0022FE78         7FFDE080         0020FE78         FFDE080           0022FE78         7FFDE080         0020FE78         00000000           0022FE78         00000000         0020FE84         00000000           0022FE84         00000000         0020FE84         00000000           0022FE80         0020FE80         0020FE80         0020FE80           0022FE90         0020FE80         0020FE80         0020FE80           0022FE84         00000000         0020FE80         00000000           0022FE84         00000000         0020FE80         00000000           0022FE84         000000000         0020FE80         <					

نقوم بعد ذلك بالضغط على زر التشغيل في البرنامج او الضغط على زر الـ F9 مرة اخرى لتخرج لنا نافذة البرنامج لإدخال الرقم (السريال نمبر) كما في الصورة التالية, أيضاً نلاحظ ان اسفل الشاشة يمين ان البرنامج في وضع التشغيل (Running).





نقوم بعد ذلك بإدخال أي قيمة كـ رقم سري في البرنامج والضغط على زر إدخال في لوحة المفاتيح للنتقل الى الصورة التالية.

C:\Users\PC\Desktop\CrackN Enter the Key:123	le.exe ad, module CrackMe]	
C File View Debug Plugins Options	Window Help	_ B ×
	→ L E M T W H C / K B R S	E . ?
Bit State         State         PUSH EBP         EBP           00121090         5         55         PUSH EBP         EBP         EBP           00121090         58         68         68861300         PUSH EBP         EBP         EBP           00121090         58         827FFFFF         CALL CrackHe.0         CALL CrackHe.0         CALL CrackHe.0           00121090         58         72851300         PUSH EBX         CALL CrackHe.0         CALL CrackHe.0           00121091         58         72851300         PUSH EAX         CALL CrackHe.0         CALL CrackHe.0           00121092         58         72851300         PUSH EAX         CALL CrackHe.0         CALL CrackHe.0           00121095         58         72851300         PUSH CrackHe.0         CALL CrackHe.0         CALL CrackHe.0           00121095         50         72813         PUSH CrackHe.0         CALL DWORD PTR           00121005         50         POP EBP         FETH         CrackHe.0         CALL DWORD PTR           00121005         50         POP EBP         FETH         CrackHe.0         FETH         CrackHe.0         FETH         CrackHe.0         FETH         CALL DWORD PTR         FETH         FETH         FETH <t< th=""><th>9136668     ASCII "Enter the Key:"       9121620     Arg2       9138678     Arg2       9138678     Crackfle.00251050       9138670     Stiller "Mabool"       9138670     Title "Mabool"       9138670     Title "Mabool"       9138670     Title "Mabool"       9138671     Title "Mabool"       9138672     Title "Mabool"       9138674     Title "Mabool"       9138694     Title "Mabool"       9138690     Text = "Invalid KEY"       9138692     DS:I(&amp;USER32.MessageBoxA       9138692     DS:I(&amp;USER32.MessageBoxA</th><th>Registers (FPU)         &lt; &lt; &lt; &lt; &lt; &lt; &lt; &lt; &lt; &lt;</th>           Registers (FPU)         &lt; &lt;</t<>	9136668     ASCII "Enter the Key:"       9121620     Arg2       9138678     Arg2       9138678     Crackfle.00251050       9138670     Stiller "Mabool"       9138670     Title "Mabool"       9138670     Title "Mabool"       9138670     Title "Mabool"       9138671     Title "Mabool"       9138672     Title "Mabool"       9138674     Title "Mabool"       9138694     Title "Mabool"       9138690     Text = "Invalid KEY"       9138692     DS:I(&USER32.MessageBoxA       9138692     DS:I(&USER32.MessageBoxA	Registers (FPU)         < < < < < < < < < <
Stack SS:[002AFE54]=0000007B	2120710	FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 0 (GT) FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Rddress         Hex         dump         Data           00130000         00130000         00130000         00130000           00130000         00130000         00130000         00130000           00130000         00130000         00130000         00130000           00130000         00130000         00130000         00130000           00130000         00130000         00130000         00130000           001300000         00130000         00130000         00130000           001300000         00130000         00130000         00130000	Comment	032211-02         00000007E           092217-02         00200007E           092217-02         00207E50           092217-02         00207E50           092217-02         00207E50           092217-02         00000000           09221
Breakpoint at CrackMe.001210AF		Paused

كما نلاحظ في الصورة اعلاه قمنا بإدخال الرقم 123 (او أي رقم آخر) ومن ثم ضغط زر ادخال (Enter) الموجود في لوحة المفاتيح وتم توقف البرنامج كما هو موضح اسفل الصورة يمين باللون الأصفر, ووصلنا الى نقطة الكسر "Break Point" التالية في عنوان الذاكرة (001210AF).



مايهمنا الآن هما العملية الثانية والثالثة باللون الأحمر في الصورة اعلاه لنتطرق الآن لشرحهما وهم.

 1. 001210AF
 817D FC 15CD5B07
 CMP DWORD PTR SS: [EBP-4], 75BCD15

 2. 001210BD
 75 13
 JNZ SHORT CrackMe.001210D2

في العملية الثانية, عند العنوان 001010AF يتم مقارنه القيمة التي يحتويها [EBP-4] بهذه القيمة 75BCD15 :

في العملية الثالثة, عند العنوان 001210BD هذه العملية عبارة عن عملية انتقال مشروط وهي اختصاراً لـ (Jump if Not Zero) وتعني:

- اذا كانت القيمة الموجوده في [EBP-4] لاتساوي هذه القيمة 75BCD15 (ملاحظة: هذه القيمة بالنظام الست عشري (hexadecimal)) سيتم الانتقال الى عنوان الذاكرة (001010D2).
- اذا كانت القيمة الموجوده في [EBP-4] تساوي هذه القيمة 75BCD15 لن يتم الانتقال الى عنوان الذاكرة (001010D2) وسيتم تنفيذ العملية التي تليها في هذا العنوان 001010BF.

نلاحظ انه اذا تم تحويل القيمة 75BCD15 (والتي تم مقارنتها في القيمة الموجوده في الـ [EBP-4] ) من النظام الست عشري (hexadecimal) الى النظام العشري (decimal) نحصل على هذه القيمة "123456789" كما في الصورة ادناه.



Calculat	tor			- 🗆 X		
≡ Programmer						Memory
				75B (	CD15	There's nothing saved in memory
HEX DEC OCT BIN	75B CD15 123,456,789 726 746 425 0111 0101 101	1 1100 1101	0001 0101			
ų	• 0 0	QW	ORD		MS	
Lsh	Rsh	Or	Xor	Not	And	
$\uparrow$	Mod	CE	с	$\langle X \rangle$	÷	
Α	В	7	8	9	×	
С	D	4	5	6	-	
E	F	1	2	3	+	
(	)	±	0		=	

لنرى الآن ماهي القيمة الموجوده بداخل هذا المسجّل "Register" عن طريق تتبّع الصور:



💥 OllyDbg - CrackMe.exe - [CPU - main threa	d, module CrackMe]		
C File View Debug Plugins Options	Window Help		_ 8 ×
	+: LEMTWHC/KBRS	<b>*</b> ?	
001210991         \$55         PUSH EEP           00121091         8BEC         HUU EBP,ESP           00121091         8BEC         PUSH ECX           00121093         51         PUSH ECX           00121094         63         8BEC           00121094         63         82FFFFF           00121094         63         82FFFFF           00121094         63         82FFFFF           00121097         804         FC           00121097         8304         90           00121097         8304         90           00121086         63         28E61300           00121086         63         28E61300           00121086         64         700           00121086         64         200           00121086         64         200           00121086         64         200           00121086         64         200           00121086         64         200           00121086         64         200           00121086         64         200           00121086         64         200           00121086         64         2061300	<pre>s.0013B668 :.0013B668 :.0013B678 s.0013B678 s.0013B678 s.0013B677 R SSIEEP-41 0013B677 R SSIEEP-41,75BCD15 0013B677 rackHe.00121002 :.0013B677 rackHe.00121002 :.0013B677 rackHe.00121002 :.0013B684 PTR DS:[&lt;&amp;USER32.MessageBoxA rext = "Invalid KEV" hOwner = NULL rest = "Invalid KEV" hOwner = NULL rest = "Invalid KEV" hOwner = NULL</pre>	Image: Series         CPU           ERAGISTERS         (FPU)           ERAS         00000001           ECX         0002FPC0           EDX         00000000           ESX         7EPC0000           ESX         7EPC0000           ESX         7EPC0000           ESX         7EPC0000           ESX         7EPC0000           ESX         7EPC0000           ESX         7EPC00000           ESX         7EPC00000           ESX         7EPC00000           ESX         7EPC000000           ESX         7EPC000000           ESX         7EPC000000           ESX         7EPC0000000           ESX         7EPC0000000           ESX         7EPC0000000           ESX         7EPC00000000           ESX         7EPC00000000           ESX         7EPC000000000           ESX         7EPC000000000000000000000000000000000000	< < < < < Plus Minus Enter oard Ctrl+C pboard
001210E4 C. C3 REIN 001210E5 56 PUSH ESI		ST6 empty 0.0 Follow in Stack	
001210E6 • H 01 Galaiae Stack SS:[002AFE54]=0000007B		FST 0000 Cond 0 0 FCW 027F Prec NEAF View MMX registers View 3DNow! registers	
Address Hex dump Data	Comment	002AFE5C 0012129C View debug registers	
002AFE58 002AFE58 002AFE58 002AFE58 002AFE58		002AFE64 00518580 002AFE64 00518580 002AFE65 00518580 002AFE6C 00518580 002AFE6C 005080736 002AFE6C 00000000	•
0007FESS         0007FESS           0002FESS         0007FESS		0020FEF74 00000000 0020FEF7C 0022FE00 0020FEF7C 0022FE00 0020FEF8C 00000000 0020FEF8C 0000000 0020FEF8C 00020FE0C 0020FEF8C 00020FE0C 0020FEF9C 0024FE0C Pointer to next SEH record 0020FEF94 00121(220 SE handler 0022FEF94 2003357	-

قمنا بالضغط على مسجّل الـ ESP موجّة الستاك "Stack Pointer" المحدد بالمربع الأحمر الأول ومن ثم الضغط على الزر الأيمن في الفاره واختيار "Follow in Stack" في المربع الأحمر الثاني.

💥 OllyDbg - CrackMe.ex	e - [CPU - main thread	ad, module CrackMe]	
C File View Debug	Plugins Options	Window Help	_ & ×
🗁 📢 🗙 🕨 🔢 🔮	비서 원임 귀	→ LEMTWHC/KBRS	
00121051         \$ 55EC           00121033         \$ 55EC           00121034         \$ 68 68B132           00121034         \$ 68 63B132           00121034         \$ 68 63B132           00121034         \$ 68 63B132           00121034         \$ 68 63B132           00121041         \$ 69 72B132           00121042         \$ 834FFFF           00121042         \$ 834FFFF           00121042         \$ 8845FFF           00121042         \$ 8845FFF           00121045         \$ 64 00           00121045         \$ 64 00           00121045         \$ 64 00           00121045         \$ 64 00           00121045         \$ 64 246132           00121045         \$ 56 772B132           00121045         \$ 56 772B132           00121045         \$ 56 972000           00121045         \$ 50 972000           00121045         \$ 50 972000           00121045         \$ 50 9720000           00121045         \$ 50 9720000           \$ 51 00204FE541=00	PUSH         EBP         SP           10         PUSH         EBP         SP           11         PUSH         ECX         PUSH         ECX           12         PUSH         CALL         CrackHe         EA         EA           16         CALL         CrackHe         EA         EA         EA         EA           18         PUSH         EAX         EAX	Image: Stress and Stres and Stress and Stress and Stress and Stress	< < <
Address Hex dump	Data	Comment 0020F13531 00000078 0020F500	A
0020FES8           0020FES8 <t< th=""><th></th><th>0020FFESC         00121220C         RETURN to CrackHe.0012129C from Cr           0020FFESC         00000001         00000001           0020FFESC         0051EE08         0051EE08           0020FFESC         00000000         0051EE08           0020FFESC         00000000         0002FFESC           0020FFESC         00000000         002FFESC           0020FFESC         00000000         002FFESC           0020FFESC         00000000         00000000           0020FFESC         000000000         00000000           0020FFESC         000000000         00000000           0020FFESC         000000000         00000000           0020FFESC         000000000         000000000           0020FFESC         000000000         000000000           0020FFESC         000000000         000000000           0020FFESC         000000000         000000000           0020FFESC         00000000000000         000000000000000000000000000000000000</th><th>aokMe.00121</th></t<>		0020FFESC         00121220C         RETURN to CrackHe.0012129C from Cr           0020FFESC         00000001         00000001           0020FFESC         0051EE08         0051EE08           0020FFESC         00000000         0051EE08           0020FFESC         00000000         0002FFESC           0020FFESC         00000000         002FFESC           0020FFESC         00000000         002FFESC           0020FFESC         00000000         00000000           0020FFESC         000000000         00000000           0020FFESC         000000000         00000000           0020FFESC         000000000         00000000           0020FFESC         000000000         000000000           0020FFESC         000000000         000000000           0020FFESC         000000000         000000000           0020FFESC         000000000         000000000           0020FFESC         00000000000000         000000000000000000000000000000000000	aokMe.00121

لنحصل على هذه القيمة الموضحة بالصورة اعلاه بالمربع الأحمر.



Calculato	r					- 🗆 X
≡	Progra	mmer	•	Memory		
					7B	There's nothing saved in memory
HEX 78 DEC 12 OCT 17 BIN 01	3 23 73 111 1011					
	<b>.</b> .	QW	ORD		MS	
Lsh	Rsh	Or	Xor	Not	And	
$\uparrow$	Mod	CE	с	$\otimes$	÷	
А	В	7	8	9	×	
с	D	4	5	6	<u>. — </u> ;	
E	F	1	2	3	+	
(	)	±	0	4	=	

وعند تحويل القيمة الموجودة في مسجّل الـ EBP من النظام الست عشري (hexadecimal) الى النظام العشري (decimal) نحصل على القيمة في الصورة اعلاه ولايلزم وجود الأصفار.



نلخص ذلك بانه في العملية الثانية عند العنوان 001210AF. يتم مقارنة الرقم "123456789" بالرقم المدخل سابقاً "123" مايعني:

في العملية الثانية, عند العنوان 001010AF يتم مقارنه الرقم "123، بالرقم "123456789"

في العملية الثالثة, عند العنوان 001210BD :

- اذا كانت القيمة 123 لاتساوي 123456789 سيتم الانتقال الى عنوان الذاكرة (001010D2) وهي رسالة الخطأ.
- اما اذا كانت القيمة المدخلة 123 تساوي 123456789 لن يتم الانتقال الى عنوان الذاكرة (001010D2)(رسالة الخطأ) وسيتم تنفيذ العملية التي تليها في هذا العنوان 001010BF مما سوف يعطينا رسالة ان رقم السريال نمر صحيح.

ونكون بذلك حصلنا على الرقم السري او السريال نمبر الخاص بالبرنامج.

في الطريقة الثانية سيتم التلاعب بالعمليات او الأوامر والتعديل عليها ليقبل البرنامج أي رقم سري نقوم بإدخالة. ومايهمنا هنا هي العملية الثالثة, عند العنوان 001210BD عملية الإنتقال المشروط JNZ" "SHORT CrackMe.001210D2

في برنامج الـ Olly والبرامج الأخرى المشابهة يمكننا التعديل على العمليات ويوجد اكثر من طريقة لجعل البرنامج يقبل أي رقم سري مدخل.

الطريقة الأولى يتم تعديل عملية الإنتقال المشروط "JNZ" لـ تصبح "JZ" وتعني ببساطة عكس الشرط اي انه اذا كان الرقم المدخل خاطئ سيتم إضهار الرسالة الصحيحه وهي ان الرقم السري المدخل صحيح, والطريقه الثاني مسح العملية بالكامل واضافة عملية او أمر الـ "NOP" "No Operation" وتعني لايوجد عملية وسيتم تنفيذ العملية التي تليها ومن ثم حفظ التعديلات على البرنامج وحفظة من جديد.

بما اننا وضعنا ثلاثة نقاط كسر ومن ثم بدئنا بتشغيل البرنامج عند وصول برنامج الـ Olly الى العنوان 001210AF وهي نقطة الكسر الثانية كما في الصورة التالية



🔆 OllyDbg - CrackMe.exe - [CPU - main thread, module CrackMe]								
C File View Debug Plugins Options Window Help								
	L E M T W H C / K B R S 🗄 🎬 ?							
Bit 1000 00121091 00121091         FS 55 00121095         PUSH EEP 00121095         PUSH ECX 00120095           00121091 00121092         51 00121092         63 00121092         63 00121092	663 828 828 828 828 828 828 828 828 828 82	< < < < < < < < < < < < < < < < < < <						
Address Hex dump Data Commen	nt 202AFE54 000000	7B						
0020FFES8         0020FFES8	0034FEE0 0045165 0022FFE60 0005105 0022FFE64 005165 0022FFE64 005165 0022FFE64 005165 0022FFE74 0025F0 0022FFE74 0025F0 0022FFE74 0025F0 0022FFE74 0025F0 0022FFE74 0025F0 0022FFE74 0025F0 0022FFE84 003000 0022FFE84 0032FE 0022FFE84 0032FE 0032FFE84 0032FFE84 00	RETURN to CrackHe.0012129C from CrackHe.00121 Big FF Big Big Big Big Big Big Big Big						
Breakpoint at CrackMe.001210AF								

نقوم بعد ذلك بضغط زر الفاره مرتين على الامر المكتوب بجانب نقطة الكسر الثالثة عند العنوان 001210BD والذي يبدأ ب"JNZ"

لتظهر هذه النافذة

🔆 OllyDbg - CrackMe.exe - [CPU - main thread, module CrackMe]	
C File View Debug Plugins Options Window Help	_ 8 ×
► ♥× ▶ II ₩ ₩ ₩ ₩ ₩ → → LEMTWHC/KBR…S ₩ ?	
Bellinson Billionson	- < < < <
FUW 02/F FTEC NEWR,53 Nask 111111	
Indexess         Hex dump         Data         Comment         002212521         000000027         000271550         00000000         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         000271550         00002715	rom CraokHe.00121
Breakpoint at CrackMe.001210AF	Paused



نقوم بعد ذلك بمسح حرف الـ N من الكلمة الأولى ليصبح الأمر "JZ" بدلاً من "JNZ" وتسمى هذه الطرقة التعديل المنطقي "Logic Editing" ويتم بعد ذلك حفظ التعديلات على البرنامج او بإستخدام الطريقة الثانية وهي الضغط بزر الفارة الايمن على العملية ومن ثم أختيار Binary ثم Fill with NOPs كما في الصورة التالية



لتظهر الصورة النهائية هكذا:

👷 OllyDbg - CrackMe.exe - [CPU - main thread, module CrackMe]							
C File View Debug Plugins Options	Window Help	_ 8 ×					
	→ L E M T W H C / K B R S	≡∎?					
00121091         F S5         PUSH EEP           00121091         \$88EC         PUSH EEX           00121091         \$88EC         PUSH EEX           00121091         \$63 6881380         PUSH ECX           00121091         \$63 6881380         PUSH ECX           00121091         \$63 6881380         PUSH ECX           00121091         \$63 72851380         PUSH ECX           00121092         \$63 72851380         PUSH Crackte           00121097         \$63 72851380         PUSH Crackte           00121097         \$63 72851380         PUSH Crackte           00121087         \$63 72851380         PUSH Crackte           00121086         \$90         PUSH Crack	2.00138668       ASCII "Enter the Key:"         0.00128678       Arsi = 00138678 ASCII '         2.00138670       Crackle 20251069         R SS:[EBP-4],758CD15       Style = MB_OK:MB_OPPLMC         2.00138670       Title = "Haboob"         Pro13E684       Title = "Haboob"         Pro15E684       Title = "Congratst VALID         Pro13B6690       Trext = "Invalid KEY"         2.00138690       Text = "Invalid KEY"         Pro15E684       Text = "Invalid KEY"         Pro15E684       Text = "Invalid KEY"         Pro15E684       Text = "Invalid KEY"         Pro15E680       Text = NULL         Pro15E680       Text = NULL	Registers (FPU)         < < < < < < < < <           PRX: 0000000         Construction         < < < < < < < < < < < < < < < < < < <					
Address Hex dump Data	Comment	A 0020FE54 0000078					
002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS 002AFESS		10027FESC         20012129C         RETURN to CrackHe.0012129C from CrackHe.00121           0027FESC         00000000         00000000           0027FESC         20000000         00000000           0027FESC         20000000         00000000           0027FESC         20000000         00000000           0027FESC         20000000         00000000           0027FESC         00000000         00000000           0027FESC         000000000         00000000           0027FESC         0000000000         000000000           00000000000000000000000000000					
Breakpoint at CrackMe.001210AF		Paused					



تم الانتهاء من التعديل و نلاحظ ان التعديلات على العملية اصبحت باللون الاحمر نقوم الآن بحفظ التعديلات على البرنامج بإتباع الصورة التالية.

💥 OllyDbg - CrackMe.exe - [CPU - main thread, module C	rackMe]	
C File View Debug Plugins Options Window	Help	_ 8 ×
	E M T W H C / K B R S 📰	?
D0121091 00121091 00121092         F5 S5 55         PUSH EBP PUSH ECX           00121092 00121092         55         PUSH ECX           00121092 00121092         56         632651300 CHL         PUSH ECX           00121092         E0832FFFFF E0832FFFFF         CHL         CrackHe.0013B643           00121092         E0832FFFFF         CHL         CrackHe.0013B673           00121092         6872B61300         PUSH EXX         PUSH EXX           00121092         6872B61300         PUSH EXX         PUSH EXX           00121082         6470         C15CD5007         PUSH CrackHe.0013B673           00121082         6470         C15CD5007         PUSH CrackHe.0013B672           00121082         6470         C15CD5007         PUSH CrackHe.0013B672           00121082         64872E61300         PUSH CrackHe.0013B672           00121082         6483461300         PUSH CrackHe.0013B           00121082         6834861300         PUSH CrackHe.0013B           00121082         6834861300         PUSH CrackHe.0013B           00121082         550         PUSH CrackHe.0013E           00121082         563         PUSH CrackHe.0013E           00121082         563         PUSH CrackHe.0013E           001210	ASCII "Enter the Key:" ASCII "Enter the Key:" ATTO: ACT AND ACT AN	Registers (FPU)         <
Address Hex dump Data Comme 002AFE58 002AFE58 002AFE58	Hit trace Run trace	Declaresd, addegeorge 02AFESS   002AFEAG 02AFESC   002AFEAG 02AFESC   002AFEAG 02AFESC   002AFEAG 02AFESC   002AFEAG 02AFESC   002AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 02AFEAG 002AF
002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58 002AFE58	New origin here Ctrl+Gray * Go to Follow in Dump Search for	BCHFEbet         B051BE80           BCHFESE         CB51BE80           BCHFESE         CB30778F           BCHFESE         CB30708F           BCHFESE         CB0000000
Breakpoint at CrackMe.001210AF	Find references to	Paused
	Copy to executable	Selection
	Analysis	All modifications
	Analysis P	Air mouncations
	Dump debugged process	

بعد الضغط على الخيار سيتم فتح نافذة جديدة نقوم بالضغط على الزر الايمن واختيار Save file

D         File         View         Debug         Plugins         Options         Window         Help           Image: Constraint of the state of the sta	Image: state sta				
Image: Weight of the second					
000004ED         90         NOP           000004EF         68 8464100         NOP           000004EF         68 90         PUSH 418684           000004EF         67 80         PUSH 41000           000004EF         67 80         PUSH 410584           000004CF         67 80         PUSH 410584           000004CF         75 80         DOE DESP.           000004CF         86E5         TOUE ESP. EBP	•				
0000004FF 68 34564100 PUSH 418584 000004FF 68 34564100 PUSH 418584 00000404CF 63 00 000004CF C 3303 000004CF C 3303 000004CF 585E HOUE ESP, EEP Copy					
00000405 FF15 10614100 CHL DUDKD 91K DS14151101 00000405 3300 XOR EAX,EAX 00000045 B8E5 HOU ESS,EBP					
00000400 50 POP EBP 00000401 C3 RETN Binary					
000004022 66 9CB64100 PUSH 41B69C 00000402 66 9CB64100 PUSH 90 Assemble					
00000409 FF15 10614100 CALL DU0RD PTR DS:[416110] 0000040F 33C0 XOR ERX,EAX Search for ►					
000004E3 50 POP EBP 000004E4 C3 RETM					
00000455 55 PUSH ESI 00000455 55 B Diracoppe FVSH incorption Go to offset Ctrl+G					
199994ED ES 35950909 CALL 90090627 099094ED ES 35950909 FIGH 90090627					
000004F8 E8 E17F0000 CALL 00008409 000004F8 E8 S510000 CALL 00008632					
000004FD 38F90 HOV E31,ERX 000004FF E8 20050000 CALL 00000A24 Hex					
000000556 09001 FUOT DUROP DTR DS: LESIJ,EAX Text ►					
000000510 3804 000 ESP 00 ESP 00 000 ESP 00 000 000 000 000 000 000 000 000 00					
00000511 54C0 TEST AL,AL 000000511 74 5C JE SHORT 00000581 Long ►					
00000517 ESE27070000 CALL 00000C43 00000517 ESE27070000 CALL 00000C43 00000517 ESE27070000 PISH 4105F					
000000521 E8 45046080 CALL 0000056F 000000525 E8 F5840000 CALL 0000056F 000000525 U Disassemble					
00000052D 50 POP EXX 0000052C E8 8F790000 CALL 00007EC0 C0 00000511 59 POP ECX					
00000532 59 POP ECX 00000532 550 TEST ERX ERX					
Udpdbb/sb/ // S 4H J// SHUKI Udpdbb/S1 Appendiance App					
108080521 3500 TEST EXX.ERV 09009541 3500 JEST EXX.ERV 09009541 JEST EXX.ERV					
00000545  68 24164000 PUSH 401624 ************************************					
0000054F 59 50F0000 CALL 0000148E	-				
Breakpoint at CrackMe.001210AF					



نقوم بإختيار الأسم الجديد للبرنامج ويتم حفظه.

CllyDbg - CrackMe ex	e - [File C\]  carr\DC\Deckton\CrackMaleve]	
D File View Deleve		
File view Debug	Plugins Options window Help	- 6' ×
	•••••••••••••••••••••••••••••••••••••	
000004BD 90 000004BE 90	NOP NOP	A
000004BF 68 84B64100	PUSH 41B684	
000004C6 FF15 1061410	a CALL_DWORD PTR DS:[416110]	
000004CE 88E5	XUR LHX, LHX MOV ESP.EBP	
000004D0 5D 000004D1 C3	POP EBP	
000004D2 68 9CB64100	PUSH 41869C	
000004D9 FF15 1061410	a CALL_DWORD_PTR DS:[416110]	
000004E1 88E5	XUR LHX, LHX MOV ESP, EEP	
000004E3 5D 000004E4 C3	POP EBP RETN	
000004E5 56 000004E6 60 01	PUSH ESI PUSH 1	
000004E8 E8 20760000		
000004F2 50	PUSH ERX	
000004F3 E8 E17F0000 000004F8 E8 35810000	CRLL 00008409 CRLL 00008632	
000004FD 88F0 000004FE F8 20050000	MOV EST,EAX	
00000504 6A 01	PUSH 1 MOU DWOPD PTP Devrett For	
00000508 E8 C1020000		
00000510 5E	HOP ES 🚜 Save file as	
00000511 84C0 00000513 ~74 6C		
00000515 DBE2 00000517 E8 27070000		
0000051C 68 6E184000 00000521 E8 4904000	PUSH 4	
00000526 E8 F5040000	opLL a File name: CrackWeAnyPassword.exe	
0000052C E8 8F790000	CALL S Save as type: Executable file (*.exe)	
00000532 59		
00000533 85C0 00000535 ~75 4A		
00000537 E8 F1040000 0000053C E8 36050000	CALL 8 Save Cancel	
00000541 85C0 00000543 774 08		
00000545 68 24164000	PUSH 347524	
0000054F 59	POPLEXX DEC	
00000555 E8 340F0000		Ψ.
Breakpoint at CrackMe.001	210AF	Paused

الآن عند تشغيل البرنامج الذي قمنا بحفظة وادخال اي رقم سري تضهر لنا الرسالة الصحيحة كما في الصورة التالية:

C:\Users\PC\Desktop\CrackMeAnyPassword.exe	
Enter the Key:123	4 III
Haboob	
Congrats! VALID KEY!!	
ОК	
	-

إلى هنا ينتهي هذا الدرس.