

# Abex crakme

---

SCP 20학번 박준형

# 목차

table of contents

- 1 crackme 란?
- 2 기본적인 Ollydbg 명령어
- 3 abex' crackme 실습
- 4 느낀점 및 Q&A

# Crackme 란?

## Part 1 Crackme란?

- Crackme란 프로그램은 말그대로 크랙 연습 목적으로 작성되어 공개된 프로그램입니다.
- 리버싱을 처음 시작할 때 간단한 crackme를 분석해보면 실제로 디버거와 디스어셈 코드에 익숙해질 수 있습니다.

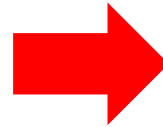
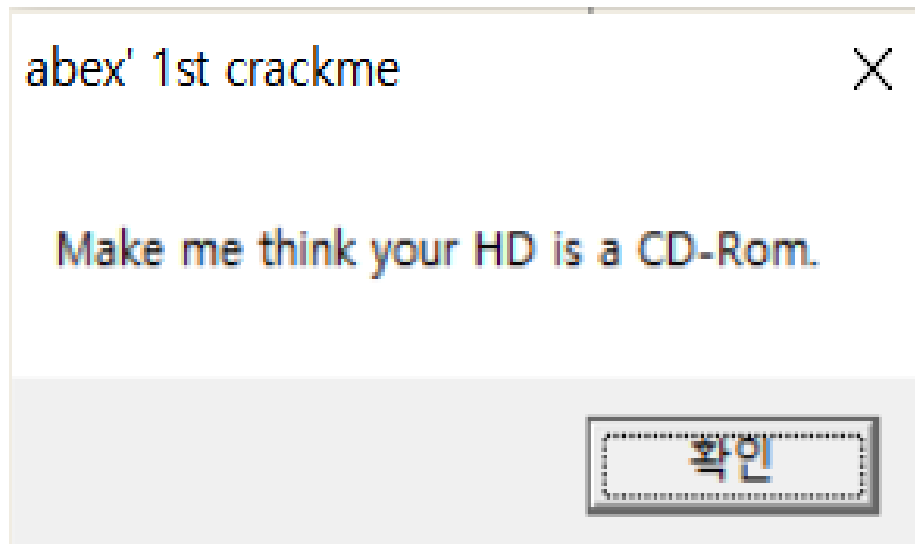
# 기본적인 Ollydbg 명령어

## Part 2 기본적인 Ollydbg 명령어

명령어	설명
PUSH	스택에 값을 입력
CALL	지정된 주소의 함수를 호출
INC	값을 1 증가
DEC	값을 1 감소
JMP	지정된 주소로 점프
CMP	주어진 두개의 피연산자 비교
JE	조건 분기(Jump if equal)

**abex' crackme 실습**

### Problem



### Result





## Part 3 abex' crackme 실습

```

CPU - main thread, module abexcm1-
00401000 $ 6A 00 PUSH 0
00401002 . 68 00204000 PUSH abexcm1-.00402000
00401007 . 68 12204000 PUSH abexcm1-.00402012
0040100C . 6A 00 PUSH 0
0040100E . E8 4E000000 CALL <JMP.&USER32.MessageBoxA>
00401013 . 68 94204000 PUSH abexcm1-.00402094
00401018 . E8 38000000 CALL <JMP.&KERNEL32.GetDriveTypeA>
0040101D . 46 INC ESI
0040101E . 48 DEC EAX
0040101F . EB 00 JMP SHORT abexcm1-.00401021
00401021 > 46 INC ESI
00401022 . 46 INC ESI
00401023 . 48 DEC EAX
00401024 . 3BC6 CMP EAX,ESI
00401026 . 74 15 JE SHORT abexcm1-.0040103D
00401028 . 6A 00 PUSH 0
0040102A . 68 35204000 PUSH abexcm1-.00402035
0040102F . 68 3B204000 PUSH abexcm1-.0040203B
00401034 . 6A 00 PUSH 0
00401036 . E8 26000000 CALL <JMP.&USER32.MessageBoxA>
0040103B . EB 13 JMP SHORT abexcm1-.00401050
0040103D > 6A 00 PUSH 0
0040103F . 68 5E204000 PUSH abexcm1-.0040205E
00401044 . 68 64204000 PUSH abexcm1-.00402064
00401049 . 6A 00 PUSH 0
0040104B . E8 11000000 CALL <JMP.&USER32.MessageBoxA>
00401050 > E8 06000000 CALL <JMP.&KERNEL32.ExitProcess>
00401055 $-FF25 50304000 JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA
0040105B .-FF25 54304000 JMP DWORD PTR DS:[<&KERNEL32.ExitProcess
00401061 $-FF25 5C304000 JMP DWORD PTR DS:[<&USER32.MessageBoxA>

[Style = MB_OK|MB_APPLMODAL
Title = "abex' 1st crackme"
Text = "Make me think your HD is a CD-Rom."
hOwner = NULL
MessageBoxA
RootPathName = "c:\\"
GetDriveTypeA

[Style = MB_OK|MB_APPLMODAL
Title = "Error"
Text = "Nah... This is not a CD-ROM Drive!"
hOwner = NULL
MessageBoxA

[Style = MB_OK|MB_APPLMODAL
Title = "YEAH!"
Text = "Ok, I really think that your HD is a CD-ROM! :p"
hOwner = NULL
MessageBoxA
ExitProcess
KERNEL32.GetDriveTypeA
KERNEL32.ExitProcess
USER32.MessageBoxA

```

## Part 3 abex' crackme 실습

```
CPU - main thread, module abexcm1-  
00401000 $ 6A 00 PUSH 0  
00401002 . 68 00204000 PUSH abexcm1-.00402000  
00401007 . 68 12204000 PUSH abexcm1-.00402012  
0040100C . 6A 00 PUSH 0  
0040100E . E8 4E000000 CALL <JMP.&USER32.MessageBoxA>  
00401013 . 68 94204000 PUSH abexcm1-.00402094  
00401018 . E8 38000000 CALL <JMP.&KERNEL32.GetDriveTypeA>  
0040101D . 46 INC ESI  
0040101E . 48 DEC EAX  
0040101F . EB 00 JMP SHORT abexcm1-.00401021  
00401021 > 46 INC ESI  
00401022 . 46 INC ESI  
00401023 . 48 DEC EAX  
00401024 . 3BC6 CMP EAX,ESI  
00401026 . 74 15 JE SHORT abexcm1-.0040103D  
00401028 . 6A 00 PUSH 0  
0040102A . 68 35204000 PUSH abexcm1-.00402035  
0040102F . 68 3B204000 PUSH abexcm1-.0040203B  
00401034 . 6A 00 PUSH 0  
00401036 . E8 26000000 CALL <JMP.&USER32.MessageBoxA>  
0040103B . EB 13 JMP SHORT abexcm1-.00401050  
0040103D > 6A 00 PUSH 0  
0040103F . 68 5E204000 PUSH abexcm1-.0040205E  
00401044 . 68 64204000 PUSH abexcm1-.00402064  
00401049 . 6A 00 PUSH 0  
0040104B . E8 11000000 CALL <JMP.&USER32.MessageBoxA>  
00401050 > E8 06000000 CALL <JMP.&KERNEL32.ExitProcess>  
00401055 $-FF25 50304000 JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA  
0040105B .-FF25 54304000 JMP DWORD PTR DS:[<&KERNEL32.ExitProcess  
00401061 $-FF25 5C304000 JMP DWORD PTR DS:[<&USER32.MessageBoxA>  
[Style = MB_OK|MB_APPLMODAL  
Title = "abex' 1st crackme"  
Text = "Make me think your HD is a CD-Rom."  
hOwner = NULL  
MessageBoxA  
RootPathName = "c:\  
GetDriveTypeA  
← EP (Entry Point)  
[Style = MB_OK|MB_APPLMODAL  
Title = "Error"  
Text = "Nah... This is not a CD-ROM Drive!"  
hOwner = NULL  
MessageBoxA  
[Style = MB_OK|MB_APPLMODAL  
Title = "YEAH!"  
Text = "Ok, I really think that your HD is a CD-ROM! :p"  
hOwner = NULL  
MessageBoxA  
ExitProcess  
KERNEL32.GetDriveTypeA  
KERNEL32.ExitProcess  
USER32.MessageBoxA
```

## Part 3 abex' crackme 실습

CPU - main thread, module abexcm1-

Address	Disassembly	Comment
00401000	PUSH 0	
00401002	PUSH abexcm1-.00402000	
00401007	PUSH abexcm1-.00402012	
0040100C	PUSH 0	
0040100E	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401013	PUSH abexcm1-.00402094	
00401018	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	INC ESI	
0040101E	DEC EAX	
0040101F	JMP SHORT abexcm1-.00401021	
00401021	INC ESI	
00401022	INC ESI	
00401023	DEC EAX	
00401024	CMP EAX,ESI	
00401026	JE SHORT abexcm1-.0040103D	
00401028	PUSH 0	
0040102A	PUSH abexcm1-.00402035	
0040102F	PUSH abexcm1-.0040203B	
00401034	PUSH 0	
00401036	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040103B	JMP SHORT abexcm1-.00401050	
0040103D	PUSH 0	
0040103F	PUSH abexcm1-.0040205E	
00401044	PUSH abexcm1-.00402064	
00401049	PUSH 0	
0040104B	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401050	CALL <JMP.&KERNEL32.ExitProcess>	ExitProcess
00401055	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA	KERNEL32.GetDriveTypeA
0040105B	JMP DWORD PTR DS:[<&KERNEL32.ExitProcess	KERNEL32.ExitProcess
00401061	JMP DWORD PTR DS:[<&USER32.MessageBoxA>	USER32.MessageBoxA
00401067	DB 00	
00401068	DB 00	
00401069	DB 00	
0040106A	DB 00	

abex' 1st crackme

Make me think your HD is a CD-Rom.

확인

Style = MB\_OKIMB\_APPLMODAL  
Title = "abex' 1st crackme"  
Text = "Make me think your HD is a CD-Rom."  
hOwner = NULL  
RootPathName = "c:\  
GetDriveTypeA

Style = MB\_OKIMB\_APPLMODAL  
Title = "Error"  
Text = "Nah... This is not a CD-ROM Drive!"  
hOwner = NULL  
eBoxA

Style = MB\_OKIMB\_APPLMODAL  
Title = "YEAH!"  
Text = "Ok, I really think that your HD is a CD-ROM! :p"  
hOwner = NULL  
eBoxA

ExitProcess

## Part 3 abex' crackme 실습

CPU - main thread, module abexcm1-

Address	Disassembly	Comment
00401000	PUSH 0	
00401002	PUSH abexcm1-.00402000	
00401007	PUSH abexcm1-.00402012	
0040100C	PUSH 0	
0040100E	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401013	PUSH abexcm1-.00402094	
00401018	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	INC ESI	
0040101E	DEC EAX	
0040101F	JMP SHORT abexcm1-.00401021	
00401021	INC ESI	
00401022	INC ESI	
00401023	DEC EAX	
00401024	CMP EAX,ESI	
00401026	JE SHORT abexcm1-.0040103D	
00401028	PUSH 0	
0040102A	PUSH abexcm1-.00402035	
0040102F	PUSH abexcm1-.0040203B	
00401034	PUSH 0	
00401036	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040103B	JMP SHORT abexcm1-.00401050	
0040103D	PUSH 0	
0040103F	PUSH abexcm1-.0040205E	
00401044	PUSH abexcm1-.00402064	
00401049	PUSH 0	
0040104B	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401050	CALL <JMP.&KERNEL32.ExitProcess>	ExitProcess
00401055	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA	KERNEL32.GetDriveTypeA
0040105B	JMP DWORD PTR DS:[<&KERNEL32.ExitProcess	KERNEL32.ExitProcess
00401061	JMP DWORD PTR DS:[<&USER32.MessageBoxA>	USER32.MessageBoxA
00401067	DB 00	
00401068	DB 00	
00401069	DB 00	

Style = MB\_OK|MB\_APPLMODAL  
Title = "abex' 1st crackme"  
Text = "Make me think your HD is a CD-Rom."  
hOwner = NULL  
RootPathName = "c:\  
GetDriveTypeA

Style = MB\_OK|MB\_APPLMODAL  
Title = "Error"  
Text = "Nah... This is not a CD-ROM Drive!"  
hOwner = NULL  
geBoxA

Style = MB\_OK|MB\_APPLMODAL  
Title = "YEAH!"  
Text = "Ok, I really think that your HD is a CD-ROM! :p"  
hOwner = NULL  
er = NULL  
MessageBoxA  
ExitProcess

Error

Nah... This is not a CD-ROM Drive!

확인



## Part 3 abex' crackme 실습

00401013	. 68 94204000	PUSH abexcm1-.00402094	[RootPathName = "c:\"
00401018	. E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	[GetDriveTypeA
0040101D	. 46	INC ESI	
0040101E	. 48	DEC EAX	
0040101F	. EB 00	JMP SHORT abexcm1-.00401021	
00401021	> 46	INC ESI	
00401022	. 46	INC ESI	
00401023	. 48	DEC EAX	
00401024	. 3BC6	CMP EAX,ESI	
00401026	> 74 15	JE SHORT abexcm1-.0040103D	
00401028	. 6A 00	PUSH 0	[Style = MB_OKIMB_APPLMODAL
0040102A	. 68 35204000	PUSH abexcm1-.00402035	Title = "Error"
0040102F	. 68 3B204000	PUSH abexcm1-.0040203B	Text = "Nah... This is not a CD-ROM Drive!"
00401034	. 6A 00	PUSH 0	hOwner = NULL
00401036	. E8 26000000	CALL <JMP.&USER32.MessageBoxA>	[MessageBoxA
0040103B	. EB 13	JMP SHORT abexcm1-.00401050	
0040103D	> 6A 00	PUSH 0	[Style = MB_OKIMB_APPLMODAL
0040103F	. 68 5E204000	PUSH abexcm1-.0040205E	Title = "YEAH!"
00401044	. 68 64204000	PUSH abexcm1-.00402064	Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049	. 6A 00	PUSH 0	hOwner = NULL
0040104B	. E8 11000000	CALL <JMP.&USER32.MessageBoxA>	[MessageBoxA
00401050	> E8 06000000	CALL <JMP.&KERNEL32.ExitProcess>	[ExitProcess
00401055	-\$FF25 50304000	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA	KERNEL32.GetDriveTypeA
0040105B	-\$FF25 54304000	JMP DWORD PTR DS:[<&KERNEL32.ExitProcess	KERNEL32.ExitProcess
00401061	-\$FF25 5C304000	JMP DWORD PTR DS:[<&USER32.MessageBoxA	USER32.MessageBoxA

## Part 3 abex' crackme 실습

00401000	\$ 6A 00	PUSH 0
00401002	. 68 00204000	PUSH abexcm1.00402000
00401007	. 68 12204000	PUSH abexcm1.00402012
0040100C	. 6A 00	PUSH 0
0040100E	. E8 4E000000	CALL <JMP.&USER32.MessageBoxA>
00401013	. 68 94204000	PUSH abexcm1.00402094
00401018	. E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>
0040101D	. 46	INC ESI
0040101E	. 48	DEC EAX
0040101F	✓ EB 00	JMP SHORT abexcm1.00401021
00401021	> 46	INC ESI
00401022	. 46	INC ESI
00401023	. 48	DEC EAX
00401024	. 3BC6	CMP EAX,ESI
00401026	✓ 74 15	JE SHORT abexcm1.0040103D
00401028	. 6A 00	PUSH 0
0040102A	. 68 35204000	PUSH abexcm1.00402035
0040102F	. 68 3B204000	PUSH abexcm1.0040203B
00401034	. 6A 00	PUSH 0
00401036	. E8 26000000	CALL <JMP.&USER32.MessageBoxA>
0040103B	✓ EB 13	JMP SHORT abexcm1.00401050
0040103D	> 6A 00	PUSH 0
0040103F	. 68 5E204000	PUSH abexcm1.0040205E
00401044	. 68 64204000	PUSH abexcm1.00402064
00401049	. 6A 00	PUSH 0
0040104B	. E8 11000000	CALL <JMP.&USER32.MessageBoxA>
00401050	> E8 06000000	CALL <JMP.&KERNEL32.ExitProcess>
00401055	\$-FF25 50304000	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA>]
0040105B	\$-FF25 54304000	JMP DWORD PTR DS:[<&KERNEL32.ExitProcess>]
00401061	\$-FF25 5C304000	JMP DWORD PTR DS:[<&USER32.MessageBoxA>]
00401067	00	DB 00
00401068	00	DB 00
00401069	00	DB 00
0040106A	00	DB 00

> 이 두 명령어를 실행하지 않아야 함

Registers (FPU)				<	<	<	<
EAX	00000003						
ECX	004F0000						
EDX	004F0000						
EBX	003EE000						
ESP	0019FF74						
EBP	0019FF80						
ESI	00000000						
EDI	00401000	abexcm1.<ModuleEntryPoint>					
EIP	0040101D	abexcm1.0040101D					
CS	002B	32bit 0(FFFFFFFF)					
DS	0023	32bit 0(FFFFFFFF)					
SS	002B	32bit 0(FFFFFFFF)					
ES	002B	32bit 0(FFFFFFFF)					
FS	0053	32bit 3F1000(FFF)					
GS	002B	32bit 0(FFFFFFFF)					
LastErr	ERROR_SUCCESS (00000000)						
EFL	00000246	(NO,NB,E,BE,NS,PE,GE,LE)					
ST0	empty	0.0					
ST1	empty	0.0					
ST2	empty	0.0					
ST3	empty	0.0					
ST4	empty	1.00000000000000000000					
ST5	empty	13.00000000000000000000					
ST6	empty	10.307692307692308376					
ST7	empty	-1.00000000000000000000					
FST	4020	Cond 1 0 0 0 Err 0 0 1 0 0 0 0 0 (EQ)					
FCW	027F	Prec NEAR,53 Mask 1 1 1 1 1 1					

## Part 3 abex' crackme 실습

00401000	\$ 6A 00	PUSH 0
00401002	. 68 00204000	PUSH abexcm1.00402000
00401007	. 68 12204000	PUSH abexcm1.00402012
0040100C	. 6A 00	PUSH 0
0040100E	. E8 4E000000	CALL <JMP.&USER32.MessageBoxA>
00401013	. 68 94204000	PUSH abexcm1.00402094
00401018	. E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>
0040101D	. 46	INC ESI
0040101E	. 48	DEC EAX
0040101F	✓ EB 00	JMP SHORT abexcm1.00401021 ← 수정
00401021	> 46	INC ESI
00401022	. 46	INC ESI
00401023	. 48	DEC EAX
00401024	. 3BC6	CMP EAX,ESI
00401026	✓ 74 15	JE SHORT abexcm1.0040103D
00401028	. 6A 00	PUSH 0
0040102A	. 68 35204000	PUSH abexcm1.00402035
0040102F	. 68 3B204000	PUSH abexcm1.0040203B
00401034	. 6A 00	PUSH 0
00401036	. E8 26000000	CALL <JMP.&USER32.MessageBoxA>
0040103B	✓ EB 13	JMP SHORT abexcm1.00401050
0040103D	> 6A 00	PUSH 0
0040103F	. 68 5E204000	PUSH abexcm1.0040205E
00401044	. 68 64204000	PUSH abexcm1.00402064
00401049	. 6A 00	PUSH 0
0040104B	. E8 11000000	CALL <JMP.&USER32.MessageBoxA>
00401050	> E8 06000000	CALL <JMP.&KERNEL32.ExitProcess>
00401055	\$-FF25 50304000	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA>]
0040105B	-\$-FF25 54304000	JMP DWORD PTR DS:[<&KERNEL32.ExitProcess>]
00401061	\$-FF25 5C304000	JMP DWORD PTR DS:[<&USER32.MessageBoxA>]
00401067	00	DB 00
00401068	00	DB 00
00401069	00	DB 00
0040106A	00	DB 00

Registers (FPU)		<	<	<	<
EAX	00000003				
ECX	004F0000				
EDX	004F0000				
EBX	003EE000				
ESP	0019FF74				
EBP	0019FF80				
ESI	00000000				
EDI	00401000	abexcm1.<ModuleEntryPoint>			
EIP	0040101D	abexcm1.0040101D			
C 0	ES 002B	32bit 0(FFFFFFFF)			
P 1	CS 0023	32bit 0(FFFFFFFF)			
A 0	SS 002B	32bit 0(FFFFFFFF)			
Z 1	DS 002B	32bit 0(FFFFFFFF)			
S 0	FS 0053	32bit 3F1000(FFF)			
T 0	GS 002B	32bit 0(FFFFFFFF)			
D 0					
0 0	LastErr	ERROR_SUCCESS (00000000)			
EFL	00000246	(NO,NB,E,BE,NS,PE,GE,LE)			
ST0	empty	0.0			
ST1	empty	0.0			
ST2	empty	0.0			
ST3	empty	0.0			
ST4	empty	1.00000000000000000000			
ST5	empty	13.00000000000000000000			
ST6	empty	10.307692307692308376			
ST7	empty	-1.00000000000000000000			
			3 2 1 0	E S P U 0 Z D I	
FST	4020	Cond 1 0 0 0	Err 0 0	1 0 0 0 0 0	(EQ)
FCW	027F	Prec NEAR,53	Mask	1 1 1 1 1 1	



## Part 3 abex' crackme 실습

0040100E	. E8 4E000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401013	. 68 94204000	PUSH abexcm1-.00402094	RootPathName = "c:\\"
00401018	. E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	. 46	INC ESI	
0040101E	. 48	DEC EAX	
0040101F	. EB 00	JMP SHORT abexcm1-.00401021	00401021 → 00401023 으로 바꾸면 됨
00401021	> 46	INC ESI	
00401022	. 46	INC ESI	
00401023	. 48	DEC EAX	
00401024	. 3BC6	CMP EAX,ESI	
00401026	. 74 15	JE SHORT abexcm1-.0040103D	
00401028	. 6A 00	PUSH 0	
0040102A	. 68 35204000	PUSH abexcm1-.00402035	
0040102F	. 68 3B204000	PUSH abexcm1-.0040203B	
00401034	. 6A 00	PUSH 0	
00401036	. E8 26000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040103B	. EB 13	JMP SHORT abexcm1-.00401050	
0040103D	> 6A 00	PUSH 0	
0040103F	. 68 5E204000	PUSH abexcm1-.0040205E	
00401044	. 68 64204000	PUSH abexcm1-.00402064	
00401049	. 6A 00	PUSH 0	
0040104B	. E8 11000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401050	> E8 06000000	CALL <JMP.&KERNEL32.ExitProcess>	ExitProcess
00401055	\$. FF25 50304000	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA	KERNEL32.GetDriveTypeA
0040105B	\$. FF25 54304000	JMP DWORD PTR DS:[<&KERNEL32.ExitProcess	KERNEL32.ExitProcess
00401061	\$. FF25 5C304000	JMP DWORD PTR DS:[<&USER32.MessageBoxA>	USER32.MessageBoxA

Assemble at 0040101F

JMP SHORT 00401023

☒ Fill with NOP's

Assemble Cancel



## Part 3 abex' crackme 실습

CPU - main thread, module abexcm1

Address	Disassembly	Comment
00401000	PUSH 0	
00401002	PUSH abexcm1.00402000	
00401007	PUSH abexcm1.00402012	
0040100C	PUSH 0	
0040100E	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401013	PUSH abexcm1.00402094	
00401018	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	INC ESI	
0040101E	DEC EAX	
0040101F	JMP SHORT abexcm1.00401023	
00401021	INC ESI	
00401022	INC ESI	
00401023	DEC EAX	
00401024	CMP EAX, ESI	
00401026	JE SHORT abexcm1.0040103D	
00401028	PUSH 0	
0040102A	PUSH abexcm1.00402035	
0040102F	PUSH abexcm1.0040203B	
00401034	PUSH 0	
00401036	CALL <JMP.&USER32.Message	
0040103B	JMP SHORT abexcm1.00401050	
0040103D	PUSH 0	
0040103F	PUSH abexcm1.0040205E	
00401044	PUSH abexcm1.00402064	
00401049	PUSH 0	
0040104B	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401050	CALL <JMP.&KERNEL32.ExitProcess>	ExitProcess
00401055	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTypeA	KERNEL32.GetDriveTypeA
0040105B	JMP DWORD PTR DS:[<&KERNEL32.ExitProcess	KERNEL32.ExitProcess
00401061	JMP DWORD PTR DS:[<&USER32.MessageBoxA>	USER32.MessageBoxA
00401067	DB 00	
00401068	DB 00	
00401069	DB 00	
0040106A	DB 00	

Registers (FPU)

Register	Value
EAX	00000001
ECX	004C0000
EDX	004C0000
EBX	00267000
ESP	0019FF64
EBP	0019FF80
ESI	00000001
EDI	00401000 abexcm1.<ModuleEntryPo
EIP	0040104B abexcm1.0040104B
C 0	ES 002B 32bit 0(FFFFFFFF)
P 1	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 1	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 26A000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
0 0	LastErr ERROR_SUCCESS (00000000)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,L
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 1.000000000000000000000000
ST5	empty 0.500000000000000000000000
ST6	empty 1.000000000000000000000000
ST7	empty -1.000000000000000000000000
FST	4020 Cond 1 0 0 0 Err 0 0 1 0
FCW	027F Prec NEAR,53 Mask

Style = MB\_OK|MB\_APPLM  
Title = "abex' 1st cra  
Text = "Make me think  
hOwner = NULL  
RootPathName = "c:\  
GetDriveTypeA

Style = MB\_OK|MB\_APPLM  
Title = "Error"  
Text = "Nah... This is  
hOwner = NULL  
RootPathName = NULL  
GetDriveTypeA

YEAH!  
Ok, I really think that your HD is a CD-ROM! :p

확인

17

# Q&A